STIFTUNG DATENSCHUTZ

BASIC RULES FOR THE ANONYMISATION OF PERSONAL DATA

Process Management, Evaluation and Monitoring

AUTHORS

Prof. Dr. Rolf Schwartmann, Andreas Jaspers, Dr. Niels Lepperhoff, Steffen Weiß LL.M.

Basic Rules for the Anonymisation of Personal Data

Process management, evaluation and monitoring

prepared and submitted on behalf of the Foundation for Data Protection

in December 2022

from

Professor Dr Rolf Schwartmann
Cologne Research Centre for Media Law, Cologne University of Applied Sciences,
German Association for Data Protection and Data Security (GDD) e.V.,

Andreas Jaspers, attorney-at-law
German Association for Data Protection and Data Security (GDD) e.V.,
DSZ Datenschutz Zertifizierungsgesellschaft mbH,

Dr Niels Lepperhoff
DSZ Datenschutz Zertifizierungsgesellschaft mbH,
XAMIT Bewertungsgesellschaft mbH,

Steffen Weiß, LL.M., attorney-at-law
German Association for Data Protection and Data Security (GDD) e.V.

Table of contents

1. Aim

The following basic rules were created for the Data Protection Foundation and are based on the “Practice Guide to Anonymising Personal Data".[1] They are not a code of conduct pursuant to Art. 40 of the GDPR but are intended as a generally applicable set of rules. Associations or other organisations representing data processors may develop general or sector-specific codes of conduct based on these principles if they are intended to regulate the anonymisation of personal data. In order to be approved as a code of conduct, supplements and concretisations may be required.

2. General definitions of terms

- **Anonymous data** is information that does not relate to an identified or identifiable natural person.
- **Record:** The information belonging to a person.
- **Direct identifiers:** Any information that directly enables a person to be identified (e.g. name or address).
- **Indirect identifiers:** All data that does not belong to the direct identifiers, but from which a personal reference can be made. For example, if they are unique and this information can be associated with a person.
- **K-anonymity:** A data collection provides k-anonymity if the data it still contains for each individual person matches at least k - 1 other persons. K is a natural number here.
- **Personal data:** Any information relating to an identified or identifiable natural person (Art. 4(1) GDPR).
- **Re-identification** is the determination of a natural person on the basis of an anonymised data set.

3. Scope of application of the basic rules

These basic rules apply to controllers and processors, regardless of industry or sector, when they anonymise personal data. The basic rules apply regardless of the controller's or processor's internal organisation and division of tasks. Controllers or processors who use anonymised data in their services or products can use these rules to demonstrate that the anonymised data used has been created in accordance with the rules defined herein and that re-identification during the period of use is unlikely. Data controllers and processors decide for themselves which anonymous data they want to subject to these rules. In the case of those products, services or other data processing operations that make use of anonymised data that have been anonymised in accordance with these rules, this fact shall be indicated in a transparent manner.

[1] https://stiftungdatenschutz.org/anonymisierung.

4. Requirements to be met

4.1 Organisational measures

Without prejudice to the other obligations of the GDPR for controllers and processors, the specialist anonymiser shall coordinate the individual organisational responsibilities before, during and after the implementation of anonymisation.

.

Number	Requirement
1.0	Appointment of a person responsible for anonymisation. ***Note: The** risk of re-identification of data subjects must be assessed on the basis of an anonymised data set. The assessment requires special knowledge in the field of anonymisation techniques, statistical procedures but also of the sector in which anonymisation takes place. Therefore, an expert person or department is required to carry out this assessment.*

4.2 Identification and documentation of the criteria necessary to determine the anonymisation method

The following requirements apply in the conceptual phase of anonymisation. They represent the necessary considerations in order to technically implement anonymisation in a second step (see chapter 4.3) to carry out the anonymisation technically.

Number	Requirement
2.0	Documentation of the circumstances of the processing: – Nature of the personal data processed ***Note:** All data fields that are to be anonymised must be listed.* – Intended purposes of processing ***Note:** The purposes for which the anonymised data are to be used must be described. A distinction must be made between the purposes of the controller and those of third parties.* – Legal basis ***Note:** Anonymisation constitutes a processing of personal data, which requires a legal basis under Art. 6 or 9 GDPR. The purpose of the processing must be appreciated when assessing the legal basis.*

	– Context of anonymisation based on the following parameters:
	  – Internal use of anonymised data or
	  – Disclosure to specified recipient(s)
	  – Publication
	  Note: *The knowledge and skills assumed of an attacker depend on the context of use of the anonymised data. If the data is to be made public, a deeper level of expertise and equipment can be assumed - in view of the large number of (criminal and state) actors - than if the data is to be passed on to a specific recipient.*
	– Risks for rights and freedoms of data subjects in case of re-identification
	  Note: *Description of possible risks to data subjects' rights and freedoms in the event of re-identification (e.g. loss of control over their personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy or other significant economic or social harm to the data subject).*
	– Expected number of data sets
	  Note: *The number of expected data records is important when using one or more anonymisation techniques. For example, a small number of data sets can have a negative effect on k-anonymity. The more features there are, the more data sets are needed.*
	– Identify the statistical properties in the datasets that are needed and which characteristics are relevant for these properties
	  Note: *Depending on the purpose of anonymisation, certain statistical properties are required from an originally personal data set. Anonymisation techniques change the statistical properties of the dataset to a greater or lesser extent.*
	– Suitable anonymisation procedures
	  Note: *After determining the circumstances of the processing, appropriate anonymisation procedures must be examined (for the various techniques, see the practice guide to anonymising personal data[2]).*

[2] https://stiftungdatenschutz.org/anonymisierung.

	– Determination of the appropriate anonymisation method(s) and the time of anonymisation ***Note:*** *One or more suitable methods are to be selected from existing anonymisation techniques. In addition, the point in time of anonymisation must be determined, i.e. when the transformation of personal data into anonymised data is started. The documentation of the point in time is important in order to have a starting point for the down-stream regular review of the anonymisation (see chapter 4.10).*

4.3 Conducting the anonymisation

Number	Requirement
3.0	Removal of all direct identification features.
3.1	Remove all unnecessary indirect identifiers.
3.2	Analysis of whether risks exist according to chapter 4.9 exist.
3.3	In the case of existing risks according to No. 3.2, implementation of one or more procedures of the • Randomisation • Generalisation or • those with synthetic data.
3.4	Analysis of whether risks for re-identification according to chapter 4.9 still exist.
3.5	If risks exist, application of further procedures according to No. 3.3.
3.6	Check whether the required statistical properties have been retained.
3.7	If risks of re-identification are still to be expected in order to preserve the statistical properties, further use of the data shall be discontinued.
3.8	Document the test and the result.

4.4 Disclosure of anonymised data to third parties

In the event of anonymised data being passed on to third parties, the following requirements apply.

4.4.1 General requirements

Number	Requirement
4.1	Agreement on a binding obligation for the recipient to check whether a re-identification of natural persons is possible on the basis of the anonymised data.
4.2	Disclosure only of data necessary for the purposes of the recipient. ***Note: The** more information a recipient receives, the higher the risk of re-identification of data subjects. Therefore, the data set should be reduced to the data that the recipient objectively needs to achieve its purpose.*

4.4.2 Joint controllership

Number	Requirement
5.1	Check whether there is joint controllership according to Art. 26 GDPR.
5.2	Determination of the controller responsible for carrying out anonymisation in the joint responsibility agreement pursuant to Art. 26 of the GDPR.
5.3	Determine whether and who is responsible for the regular review of anonymisation in accordance with chapter 4.10 is responsible.

4.5 Rights and role concept

Number	Requirement
6.1	Definition of at least two roles that differ from each other: – (1) Role with access authorisation to the dataset to be anonymised – (2) Role with access to the anonymised data
6.2	Non-allocation of role (1) to recipients of anonymised data ***Note:*** *Both internal and external receivers must be considered for the receivers.*

4.6 Principles relating to processing of personal data

Number	Requirement
7.1	Identify the legal basis for anonymisation.
7.2	Information of the data subjects within the framework of the information obligations according to Art. 13 and 14 GDPR about the anonymisation of their data in case of data collection with the following minimum contents: – Making the anonymisation – Purpose of anonymisation – Relevant legal basis

4.7 Unintentional/unlawful re-identification of data subjects

Number	Requirement
8.1	Documentation of a response plan in case of unintentional or unlawful re-identification of data subjects with the following minimum contents: – Verification of the existence of a legal basis for personal data processing – Assessment of a notification obligation according to Art. 33 / Art. 34 GDPR – Mandatory deletion of personal data in the absence of a legal basis ***Note:*** *It is not necessary to create a separate response plan. The response plan can be integrated into an existing process (e.g. a general incident response plan) at the controller or processor.*

4.8 Documentation

Where documentation of one or more measures is required within this Policy, the following documentation requirements apply.

Number	Requirement
9.1	The considerations made shall be justified in a way that is comprehensible to third parties. References to further documentation (records of processing activities) are permissible insofar as they make statements about the circumstances of the processing. The reference must include the specific title, storage or filing location and version of the referenced document. ***Note:*** *The documentation to be prepared in the respective section fulfils several objectives. The documentation forces the person responsible or the processor to systematically process the specifications of these basic rules. Insofar as the person responsible for anonymisation uses the input of other persons responsible for anonymisation, he or she has an information base that is always comprehensible. Furthermore, this documentation enables the person responsible to regularly check the original assumptions and to adjust them if necessary. Such an evaluation is necessary insofar as the General Data Protection Regulation requires anonymisation according to the respective state of the art or technological developments are to be included in the question of sufficient anonymisation. Furthermore, the documentation enables both the person responsible and other monitoring bodies in the company (e.g. Compliance or Internal Audit) to carry out compliance checks.*

4.9 Attacker model

Number	Requirement
10.1	Documentation of the assumptions of an attacker model with the following minimum contents: – Knowledge, means and other data sources of an attacker – Value of the data for the attacker ***Note:*** *As already mentioned in the context of documenting the circumstances of the processing of personal data, the knowledge and skills of an attacker depend on the context of use of the anonymised data. If the data is to be made public, a deeper level of expertise and equipment - in view of the multitude of (criminal and state) actors - can be*

	assumed than if the data is to be passed on to a specific recipient.
10.2	Carry out the risk assessment with the following test steps: – Singling out a natural person – Linking data sets – Derivation of characteristics (inference)
10.3	If anonymised data is used to train algorithms, the attacker model must also be applied to the trained algorithm. It must be checked whether the result calculated by the algorithm can lead to re-identification.

4.10 Regular review

Number	Requirement
11.1	Documentation of the inspection interval based on a risk assessment of what harm re-identification could mean for the persons concerned.
11.2	Carrying out and documenting within the scope of the check interval whether there are risks for the re-identification of natural persons in the anonymised data set. To be taken into account are: – Circumstances of processing according to chapter 4.2 – Existing means at the controller or processor (legal, technical and organisational) – Generally available technology according to the state of the art – General technological developments – The attacker model according to chapter 4.9.

5. Monitoring by the monitoring body

Pursuant to Art. 40(4) of the GDPR, procedures must be in place to enable a supervisory authority to monitor that the provisions of the policy rules are complied with.

5.1 Duty to cooperate

Participation shall include, in particular, that

1. the requested documents and evidence are provided in good time,
2. required information is provided in a timely manner,
3. there is an unrestricted right of access for employees and agents of the supervisory authority to the premises of the self-obligated undertaking, insofar as anonymisation is concerned, its processor and all other sub-processors, as well as all other places where data are processed for anonymisation or accessed from these data, and
4. staff and agents of the Authority have access to all personal data and information relevant to anonymisation, data processing facilities and equipment or processing operations in relation to this Policy.

The self-obligated undertaking undertakes to comply with the orders of the supervisory authority within the framework of its tasks pursuant to Article 41 of the GDPR, within the framework of the contractual agreements and within the framework of the powers set out in these basic rules.

5.2 Cooperation obligations of other controllers and processors

The self-committed undertaking shall ensure by an individual contractual agreement that (further) processors and other controllers jointly responsible for the processing with the self-committed undertaking are subject to the same obligations to cooperate in and tolerate control actions of the supervisory authority as itself. The foregoing shall apply only to the extent that such entities cooperate in the anonymisation or re-identification control.

5.3 Powers of the monitoring body

The self-committed company fully supports the monitoring agency. It fully recognises the following powers of the monitoring agency to which it submits:

1. Verification that the requirements for participation as described in these Basic Rules as well as in the application and in the voluntary commitment to these Basic Rules are fulfilled,
2. Acceptance or rejection of participation in the voluntary commitment to these basic rules,
3. if there are indications of a suspected violation of the basic rules, to request the companies/processors concerned to submit a statement,
4. temporarily suspend participation in the policy rules,
5. exclude the company/processor from participating in the ground rules,
6. carry out on-site inspections or have them carried out,
7. to request proof documents, in particular in the form of sample contracts to be submitted, process descriptions, etc. on compliance with the basic rules,
8. inform the data protection supervisory authority of the exclusion from the policy rules,
9. to publish the participation in the policy,

10. to set reasonable deadlines for reaction and rectification,
11. directly to the management of obligated companies/processors,
12. to approach the highest level of management in the case of a group of companies.

5.3.1 Process: Control of the voluntary commitment

The inspection of the obligated companies by the monitoring body shall be carried out as follows:

No.	Monitoring office	Company
1	2x per year: at least 5% of the companies are to be randomly selected; independently of this, at least one company is to be selected per year; minimum interval between these random inspections of the same company: 2 years. The first random audit shall take place at the earliest 2 years after the initial audit carried out in the context of the application. A mandatory audit shall take place after 7 years at the latest. If only one or two companies have signed up to the rules, they will be checked every 2 years. In addition, companies that have been temporarily suspended within the last 12 months are selected for inspection, even if the last inspection was less than 2 years ago.	
2	Require appropriate evidence of compliance (e.g. model contracts, process descriptions, etc.).	
3		Sending the requested evidence within 4 weeks.
4	If none or not all of the requested evidence is submitted, send a reminder with a deadline of 2 weeks.	
5		Send missing proofs within 2 weeks.
6	Check for evidence of compliance.	
7	If no, continue with no. 10.	
8	If yes, document result and inform company/processor.	

9	Process End.	
10	Start process "Sanctions in case of violation of the voluntary commitment".	

5.3.2 Process: Sanctions for violation of the voluntary commitment

No.	Monitoring office	Company
1	Description of the injury and answers to the questions: – What was done? – What should have been done according to the policy rules?	
2	Check whether the notification obligation under Art. 33 of the GDPR could be triggered.	
3	If obviously no, continue with 7.	
4	If yes, request a copy of the notification to affected principals (if relevant) or the competent data protection supervisory authority from the obligated company.	
5		Send a copy of the notification to affected clients (if relevant) or the competent data protection supervisory authority without delay, at the latest within 7 days.
6	If the copy or justification of non-reporting is not received within 7 days, continue with 14.	
7	Request for immediate cessation of the violation or confirmation that there is no violation within two weeks.	
8		Immediately shut down and send corresponding evidence to the monitoring agency within 2 weeks. Alternatively: Within 2 weeks, explain why there is no violation.
9	If the deadline passes, continue with step 14.	
10	Examine evidence of rectification or argumentation as to why there is no breach. In the case of serious breaches or if the rectification cannot be established or assessed effectively without an on-site inspection or on the basis of documents and information to be requested,	

	an on-site inspection may be carried out or further documents and information may be requested.	
11	If rectification is not sufficient, continue with 14.	
12	Notification to company that rectification is satisfactory and procedure is completed. In addition, if complaints triggered the process: Notification to the complainant about remedying the violation of these basic rules. Internal documentation of the communication to the company and complainant.	
13	Process End.	
14	If the second deadline is not met, continue with step 17. If the third deadline is unsuccessful, continue with step 21.	
15	If the company does not rectify or has already made an unsuccessful attempt to rectify or does not send the copy of the notification/justification of non-notification (No. 4) in time, setting of a 2nd deadline for the fulfilment of the outstanding reaction or rectification of 14 days.	
16		Reaction or successful rectification and proof thereof must be sent to the monitoring body within 14 days.
17	If the company responds appropriately, then – after sending the copy of the notification, continue with step 7, – after the breach has been remedied or the company has explained why there is no breach, proceed to step 10.	
18	If the company does not respond appropriately, then set a final deadline of 3 days.	
19		Reaction or successful rectification and proof of the same must be sent to the monitoring body within 3 days.
20	If the company responds appropriately, then	

	– after sending the copy of the notification, continue with step 7, – after the breach has been remedied or the company has explained why there is no breach, proceed to step 10.	
21	Start process "Information of the supervisory authority in case of withdrawal of voluntary commitment	
22	Exclusion from self-commitment until the violation is stopped plus prohibition to advertise with self-commitment. Information of the company about it. Information of the complainant, if available.	
23	Start process "Publication of obligated companies	
24		Remove reference to the voluntary commitment from all advertising and other materials within 4 weeks.

The company is entitled to make a one-time substantiated request for an extension of the deadline specified in step 8 to 8 weeks. The monitoring body decides at its own discretion whether the extension of the deadline is granted. If yes, the extended deadline applies to step 9.

The decision on what consequences to draw from a breach is at the discretion of the monitoring body. The monitoring agency shall make decisions at its own discretion to suspend or withdraw the voluntary commitment. The (temporary) withdrawal of a voluntary commitment during the term of the contract does not terminate the contractual relationship nor does it release from the obligations agreed in the contract.

5.4 Process: Review for breach of self-commitment in case of complaint

No.	Monitoring office	Company
1	Examination whether the complaint describes verifiable facts and identifies the infringing act ("substantive" complaint)	
2	Checking whether the substantive scope of application of the basic rules is affected by the complaint	

3	If material scope of application is not affected, inform complainant with reasons; process end	
4	If complaint is not substantive, request complainant to elaborate on facts or provide evidence of misconduct	
5	If the material scope of application is affected and the complaint is substantial, request a statement from the company within 4 weeks. In the case of suspicion of serious violations or in cases where there are indications that evidence of violations may be intentionally or unintentionally destroyed, an additional short-term on-site inspection takes place. In the case of an obvious violation of these basic rules, a temporary order to stop the infringing act may additionally be issued.	
6		Comment on the complaint within 2 weeks, explaining why the complaint is incorrect or what measures have been taken to stop the infringement.
7	If the deadline passes without a reply, send a reminder with a deadline of 2 weeks.	
8		Comment on the complaint within 2 weeks, explaining why the complaint is incorrect or what measures have been taken to stop the infringement.
9	If the company replies or if the grace period has expired, examine the facts in the light of the available statements of the complainant and the company as well as the company's own findings.	
10	In the event of an allegation of a serious breach or if the allegation cannot be assessed or cannot be assessed effectively without an on-site inspection or on the basis of documents and	

	information to be requested, an on-site inspection may be carried out or documents and information may be requested.	
11	Statement of the company proves compliance and on-site inspection carried out if necessary showed no further deficiencies: – Inform complainant – Process end	
12	Statement of the company or, if applicable, on-site inspection carried out shows deficiencies: Start process "Sanctions in case of violation of the voluntary commitment".	

5.5 Process: Informing the supervisory authority in the event of withdrawal of the voluntary commitment

No.	Monitoring office	Company
1	Drawing up and sending a letter explaining the measure and justifying it.	
2	Filing the letter	

5.6 Process: Publication of obligated companies

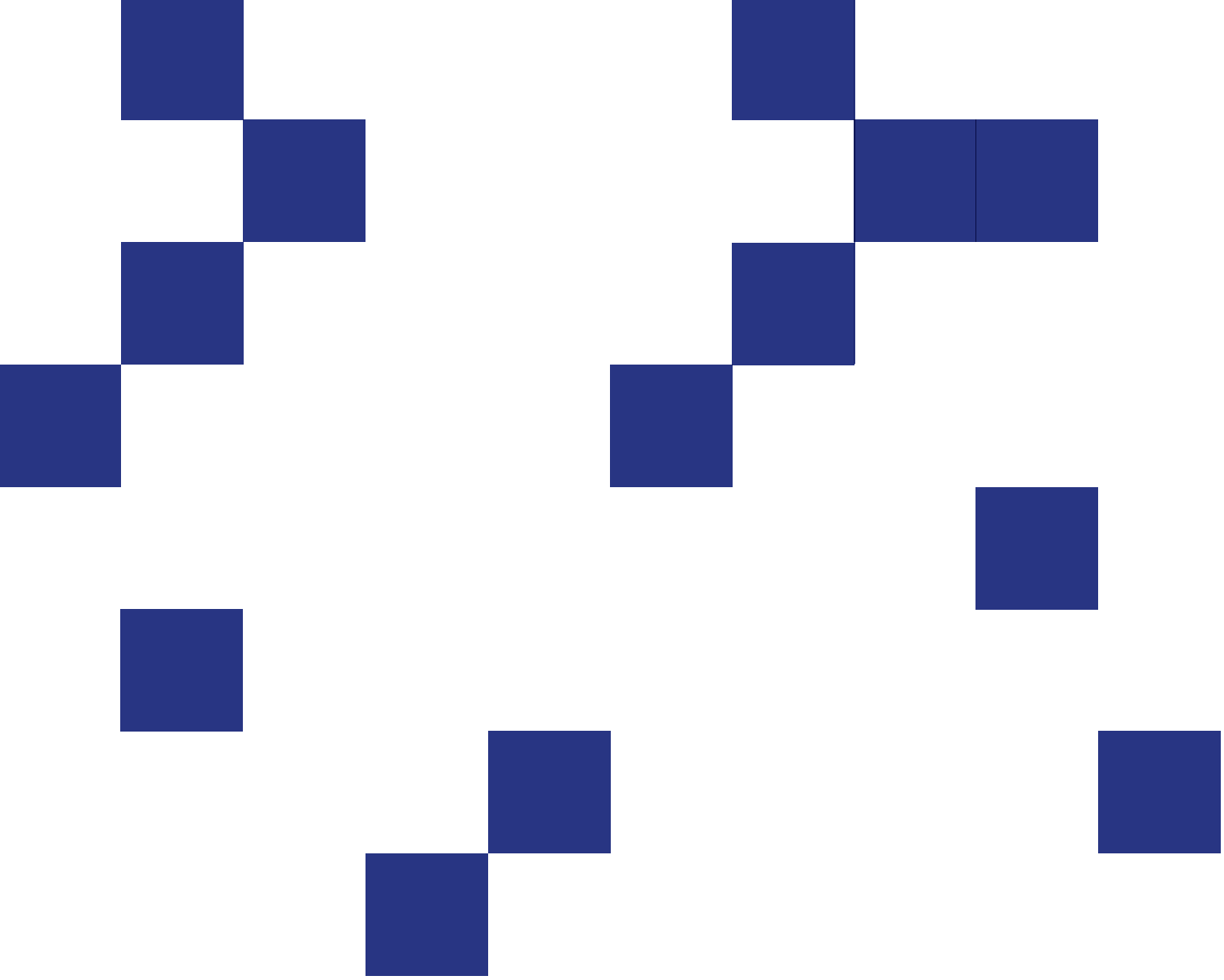
No.	Monitoring office	Company
1	Inclusion in the public directory, accessible via the website of the monitoring body, if a voluntary commitment has been issued.	

5.7 Process: Publication of suspended or withdrawn voluntary commitments

No.	Monitoring office	Company
1	In the case of temporary or permanent suspension, attach a note to the entry stating that the voluntary commitment has been temporarily or permanently suspended	

6. Process: Review of the basic rules

No.	Proprietor of the basic rules
1	The basic rules are subject to continuous monitoring with regard relevance and legal conformity. This is the responsibility of the proprietor of the basic rules. Every three years, the proprietor shall submit a written report to the competent supervisory authority, in particular on the development of dissemination, sanctions, complaints as well as any need for adjustment of the basic rules. Amendments and extensions of these basic rules shall only be effective after approval by the competent supervisory authority.



STIFTUNG
DATENSCHUTZ

Stiftung Datenschutz
foundation with legal capacity under civil law
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

T +49 341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Funded by the Federal Republic of Germany
represented by Frederick Richter (Chairman)

The work of the Stiftung Datenschutz is funded from the federal budget (BMJ section).

Federal Ministry
of Justice