

KNAUF GROUP

Data Privacy Policy

Version	1.0
Last revised	01.06.2023
Status	Resolved

GENERAL

Brief Summary	Policy for the handling of personal data in the Knauf Group
Policy Type	Group Directive
Policy Owner	Chief Compliance Officer
Policy Approver(s)	General Partners; General Counsel
Related Policies & Procedures	Knauf Global Procurement Policies, Knauf IT Policies, various data privacy guidelines & procedures
Storage Location	Knauf Intranet / Knauf DMS
Scope of Application	All Knauf Companies worldwide (Comply or Explain Principle)
Classification level	<input type="checkbox"/> public <input checked="" type="checkbox"/> internal <input type="checkbox"/> restricted <input type="checkbox"/> confidential
Date of Validity of this version (Gebr. Knauf KG)	July 01, 2023
Review Cycle	annually

REVISION HISTORY

Version ID	Date Change	of	Author	Rational

CONTENTS

1.	POLICY STATEMENT	4
2.	POLICY SUBJECT	4
2.1	Scope	4
2.2	Minimum Standard	4
2.3	Related Knauf Policies & Guidelines	4
3.	GENERAL PRINCIPLES	5
3.1	What is Personal Data?	5
3.2	The Data Privacy Principles – how Knauf shall process Personal Data.....	5
3.3	Processing of Sensitive Personal Data	6
4.	DATA SUBJECT ACCESS REQUESTS	6
5.	DATA SHARING	6
5.1	Data sharing with other Controllers.....	7
5.2	Data sharing with Processors	7
5.3	Data transfers to Third Countries	7
6.	DATA BREACHES.....	7
7.	ASSESSING PROCESSING ACTIVITIES AND RECORDKEEPING	7
7.1	ROPA	8
7.2	General assessment requirement.....	8
7.3	Data protection impact assessment	8
8.	DATA PRIVACY GOVERNANCE.....	8

1. POLICY STATEMENT

Protecting personal information relating to customers, employees and other individuals associated with the Knauf Group (the **Personal Data**) is a top priority for all affiliated companies within the Knauf Group (the Knauf Companies or Knauf). Knauf is committed to process Personal Data only in a fair, lawful, and transparent manner and to use such Personal Data for legitimate purposes only.

As part of this commitment, Knauf has established this Data Privacy Policy (the **Policy**) reflecting Knauf's global principles and standards on handling Personal Data.

2. POLICY SUBJECT

2.1 Scope

This Policy applies to all processing activities of Personal Data, such as but not limited to collecting, managing, retaining and sharing of Personal Data (**Processing Activities**) by all Knauf Companies and extends to all jurisdictions in which Knauf operates and does business. In particular, its territorial scope is not restricted to Personal Data Processing Activities of Knauf Companies within the European Economic Area (**EEA**) or UK.

For the purpose of this Policy, the relevant Knauf Companies qualify as Controllers within the meaning of Article 4 No. 7 GDPR, i.e. as entities which independently or jointly determine the purposes and means of the Processing Activities.

Knauf's employees, including managers, executives, and personnel, as well as contract and temporary workers (together referred to as **Knauf Personnel**) are responsible for compliance with this Policy and have to follow the terms and conditions set forth in this Policy at all times.

Because of the complexity of Data Privacy Laws, Knauf Personnel are highly **encouraged to consult their competent Privacy Function** (see **Data Privacy Governance Policy** for details) and/or seek external advice if they are confronted with any situation raising issues in respect of protection, privacy, or security of Personal Data.

Please also contact the competent Privacy Function or via the Knauf Speak-Up Line if you become aware of a breach of this Policy (see sec. 8).

2.2 Minimum Standard

This Policy is based on the EU General Data Protection Regulation (**GDPR**) and serves as a Minimum Standard for the protection of Personal Data across the Knauf Group. All Knauf Companies are at all times obligated to comply with any applicable data protection provisions of the country in which the Personal Data is processed (**Data Privacy Laws**). Consequently, existing local laws and regulations which individual Knauf Companies have to comply with for the processing of Personal Data that go beyond the principles laid out in this Policy, or that contain additional or different restrictions on the processing and use of Personal Data, shall remain unaffected by this Policy and take precedent. Knauf Companies located outside the EU/EEA may be exempt from the Minimum Standard based on reasons related to local legal requirements, market standards, or technical and operational difficulties. Such exemption and its reasons need to be notified and documented (**Comply or Explain Approach**). Please contact your competent Privacy Function for further details (see sec. 8).

2.3 Related Knauf Policies & Guidelines

This Policy is one of several policies that set out Knauf's approach to the handling of Personal Data and other information, including:

- Knauf Data Privacy Governance Policy
- Knauf Standard Data Deletion Concept;
- Knauf Data Breach Response Plan;
- Knauf Data Subject Request Management;
- Knauf Cookies Guideline;
- Knauf Privacy by Design & Privacy by Default Guideline;
- Knauf Global Procurement Policies;

- Knauf IT Policy; and
- Knauf IT Security Policy. (together, the **Relevant Policies**)

While this Policy is valid globally as the Minimum Standard more specific Knauf policies need to be complied with as well. If this Policy conflicts with any local laws or legislation or in case of any conflicts between local Knauf policies and this Policy, the Owner of this Policy should be informed in writing immediately. Generally, in case of contradictory other policies, this Policy takes precedent.

3. GENERAL PRINCIPLES

3.1 What is Personal Data?

Personal Data (sometimes also called "personal information" or "personally identifiable information" or "PII") for the purposes of this Policy means any information relating to an identified or identifiable living individual (**Data Subject**) as defined in Article 4 No. 1 GDPR.

Examples of Personal Data include names, dates of birth, addresses or contact details (both professional and private), signatures, identification numbers (such as for social security purposes, passports, or identity cards). It also includes personnel file numbers, user credentials, IP addresses of personal devices, individual real-time location data, health, economic, cultural, or social information about individuals, as well as expressions of opinion (such as in an HR appraisal record) if it relates to specific individuals (i.e., is not effectively anonymized such as by way of aggregation in a table for mere statistical purposes).

Personal Data may relate to individuals such as Knauf Personnel, job applicants, consumers (such as website visitors) or individual contacts at suppliers, service partners and customers.

Please note that "**pseudonymized data**", i.e. data which does not contain information which clearly identifies a person (e.g. by name or job title), also qualifies as Personal Data as long as the Data Subject can be (re-)identified by using additional information (e.g. address, date of birth, photo etc.). Only if such (re-)identification is impossible, the data will be considered as being "**anonymized**" and Data Privacy Laws will not apply.

3.2 The Data Privacy Principles – how Knauf shall process Personal Data

Knauf Companies (each a Controller for the purposes of this Policy) and all Knauf Personnel shall process Personal Data in accordance with the following key principles and this in line with Article 5 GDPR (the **Data Privacy Principles**):

- **Processing shall be fair and transparent (*Fairness and Transparency*)**. Fairness is typically achieved through transparency. Any Data Subject shall be informed according to Data Privacy Laws, including, inter alia, (i) who the responsible Controller is, (ii) who the Controller's representative is, (iii) the purpose for which its Personal Data is to be processed by the Controller (or one of its service partners commissioned as Processor).
- **Processing shall be lawful (*Lawfulness*)**. Any Processing Activity requires a legal basis. Under the GDPR, the processing of Personal Data is, inter alia, lawful if (i) the Data Subject has expressly consented to the specific processing, (ii) the processing is necessary for the performance of a contract with the Data Subject, (iii) the processing is necessary to comply with a legal obligation, (iv) the Controller has a legitimate purpose in the processing which overrides the privacy interests of the Data Subjects. More stringent requirements apply to the processing of Sensitive Data (see below). For accountability purposes, the respective legal basis should always be documented properly (e.g., in the company's records of Processing Activities or by way of a signed consent form).
- **Processing shall be for limited purposes and shall be done in an appropriate way (*Purpose Limitation*)**. Personal Data shall generally only be processed for the purposes for which it was initially collected. This also applies to Personal Data of Knauf employees. If it becomes necessary to process the Personal Data for a new purpose, the Data Subjects need to be informed and the legal basis for the new purpose needs to be reassessed.

- **Processing shall be limited to what is necessary for the intended purpose (*Data Minimization*).** The collection of Personal Data shall always be as limited as possible against the background of the intended Processing Activity. An important aspect of Data Minimization is limiting access to Personal Data on a “**need-to-know basis**”. Access to Personal Data should always be restricted to Knauf Personnel who have a specific need to access such Personal Data, usually depending on their role within Knauf. Knauf Personnel should not access Personal Data (or be able to access it) where they have no genuine business reasons for doing so.
- **Personal Data shall always be accurate and kept up to date (*Accuracy*).** It is important that the Personal Data is correct. Measures shall be implemented to check the accuracy of Personal Data at the point of collection and in regular intervals thereafter. Incorrect data shall be corrected.
- **Personal Data shall not be kept longer than necessary for the purpose it was collected (*Storage Limitation*).** Personal Data shall be destroyed or erased from Knauf IT-systems when it is no longer required for the specified Processing Activity for which it was collected unless statutory retention periods apply. Consult the Knauf Standard Deletion Concept for more details.
- **Personal Data shall always be kept secure (*Integrity and Confidentiality*).** Appropriate technical and organizational measures (*TOMs*) to protect the security, confidentiality, and integrity of Personal Data shall be taken against unlawful or unauthorized processing of Personal Data, and against the accidental loss of, or damage to Personal Data.
- **Processing and compliance with Data Privacy Laws shall be documented (*Accountability*).** Knauf needs to be in a position to demonstrate compliance with Data Privacy Laws at all times. Consult the Data Privacy Governance Policy for more details on the documentation which needs to be maintained.

3.3 Processing of Sensitive Personal Data

Certain categories of Personal Data as set out in Articles 9 and 10 GDPR (***Sensitive Personal Data***) may only be processed under strict requirements. These data include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health (including, for example, information on pregnancy, maternity, information on re-integration post illness or disability), sex life, sexual orientation, genetic or biometric data as well as information relating to criminal convictions and offences.

Within the context of the business dealings of Knauf, the processing of Sensitive Personal Data is only lawful if any of the following applies:

- the Data Subject has given explicit consent;
- the processing is necessary for fulfilling Knauf's obligations under employment and social security and social protection laws;
- the processing is necessary to protect the vital interests of the Data Subject;
- the processing is necessary for the establishment, exercise, or defense of legal claims.

4. DATA SUBJECT ACCESS REQUESTS

Under the GDPR and many other Data Privacy Laws, Data Subject have the right to request access to their Personal Data (including copies of the data) which a Knauf Company processes as well as information on the related Processing Activities (***Right of access***).

If a Knauf Company or Knauf employee receive a **Data Subject Access Request** under GDPR or another Data Privacy Law that grants a Right of access comparable to the GDPR, the competent Privacy Function (see sec. 8) shall be contacted immediately. The competent Privacy Function forwards the Data Subject Request to the relevant Knauf Company to enable Knauf to respond to the request within prescribed time limits: See the Data Privacy Governance Policy for more details.

Additional data subject rights (e.g. right to erasure) are granted by the GDPR and other data protection laws and must then be observed accordingly.

5. DATA SHARING

Any sharing of Personal Data is a Processing Activity. Data Privacy Principles (see above) apply. Further requirements need to be observed if the data recipient has its seat in a country outside the EEA.

Please note that data sharing within a group of companies such as the Knauf Group is not exempted from the Data Privacy Principles.

5.1 Data sharing with other Controllers

If Personal Data is shared with other Controllers (i.e. an independent company which is not a service provider for the data sender), the data sender must ensure that there is a valid legal basis for the sharing. Furthermore, all other Data Privacy Principles as set out above must be complied with.

In case the Personal Data is under the **joint control** of a Knauf Company and another Knauf Company / a third party, additionally a joint control agreement in line with Article 26 GDPR must be concluded. Two or more entities are **Joint Controllers** if they jointly determine the purposes and means of the processing (e.g. several Knauf Companies maintain a joint Active Directory). If you believe that a Processing Activity could constitute joint control, please contact your competent Privacy Function (see sec. 8).

5.2 Data sharing with Processors

Processors process Personal Data on behalf of and upon the instruction of a Controller. For example, service providers (such as Microsoft, Salesforce, SAP) act as Processors.

The data sender must enter into a data processing agreement (DPA) with the Processor. Article 28 GDPR contains a list of provisions which need to be included in a DPA.

In case you intend to engage a Processor, please use the templates provided by Knauf. If the Processor insists on using its own templates, please contact your competent Privacy Function for assistance (see sec. 8).

5.3 Data transfers to Third Countries

Transfers of Personal Data to countries outside the EEA (**Third Countries**) are subject to the regulations as set out in Chapter V of the GDPR.

If the European Commission has issued an adequacy decision for a certain Third Country (**Safe Third Country**, see [here](#) for an up-to-date list), no further requirements apply. However, if such adequacy decision does not exist for a recipient country (**Unsafe Third Country**), the data exporter must conclude so-called Standard Contractual Clauses with the data importer. The Standard Contractual Clauses have been adopted by the European Commission and must not be amended (see [here](#)). In some cases, additional requirements apply (e.g. if Personal Data is transferred to the USA). Please see the Data Privacy Governance Policy for more information.

6. DATA BREACHES

A **Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Typical examples of Data Breaches are hacking and phishing attacks and other kinds of data theft.

Data Breaches must be reported within 72 hours of their detection to the competent data protection authority of the affected Knauf Company. If the Data Breach may put the rights of the affected Data Subjects at risk, these also need to be notified without undue delay.

Because of the strict notification obligations, it is important that you report any Data Breach that you become aware of, immediately to Knauf IT or your competent Privacy Function (see sec. 8). Please see the Data Breach Response Plan and the Data Privacy Governance Policy for more details.

7. ASSESSING PROCESSING ACTIVITIES AND RECORDKEEPING

Knauf Personnel is required to assess commencing and ongoing Processing Activities (including as part of projects, business processes and procedures) in a formal Privacy Impact Assessment (**PIA**) and to document them in the Knauf Company's records of processing activities (**ROPA**).

7.1 ROPA

Each Knauf Company establishes and maintains an up-to-date ROPA with accurate and detailed records of all Processing Activities carried out by this particular Knauf Company, including – for each Processing Activity – details of the

- Controller (i.e., Knauf Company);
- Personal Data categories processed and affected Data Subjects;
- Purposes and justification for the Processing Activity;
- IT-assets or other technical means relied on for that Processing Activity (information to be provided by Knauf IT or Knauf Digital);
- Recipients of Personal Data (including Joint Controllers or Processors);
- Data transfers to other countries or organizations, including (contractual or other) safeguards;
- Applicable retention periods; and
- Description of TOMs.

ROPAs shall be documented and managed on Knauf's digital data privacy platform (OneTrust). The Privacy Functions are responsible for reviewing and monitoring a Knauf Company's ROPA.

7.2 General assessment requirement

Common and recurring Processing Activities (such as those relating to regular HR processes or interactions with customers in the course of ordinary business) will already have been checked and documented in the ROPA. However, if new projects or business processes are being implemented for the first time, the process owner is responsible to check any processing of Personal Data entailed and whether such processing is already covered by a Processing Activity in the company's ROPA. If not, a multi-step PIA assessment process needs to be initiated to assess compliance with Data Protection Laws. Please contact your competent Privacy Function for assistance (see sec. 8).

7.3 Data protection impact assessment

Before carrying out certain types of Processing Activities which are likely to result in an increased privacy risk to Data Subjects' interests (the **High-Risk Activities**), Knauf Companies are required to conduct a Data Protection Impact Assessment (**DPIA**). A DPIA basically is the well documented assessment of a specific Processing Activity designed to identify risks arising out of this Processing Activity and describe the technical and organizational measures necessary to mitigate those risks as far and as early as possible. A DPIA shall be carried out in case of:

- Profiling
- Processing of large amounts of Sensitive Data
- Processing of Personal Data the disclosure of which may have negative consequences for the Data Subjects, e.g. private communications data; salary data, real-time location data (GPS), passport numbers, information on disciplinary measures etc.

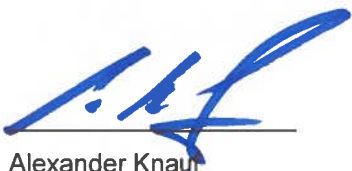
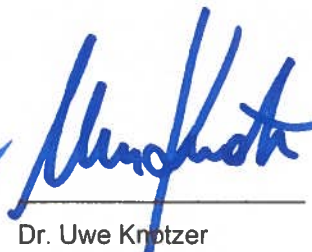
Please see the Data Privacy Governance Policy for more details.

8. DATA PRIVACY GOVERNANCE

Knauf has set-up a multi-layered data privacy governance system with dedicated Privacy Functions, such as group data protection officer, Local Privacy Coordinators and the Group Data Privacy Board. If in doubt on any instructions given in this Policy, Knauf employees should first contact the Privacy Coordinator responsible for their company, country/region, or division. Please see the Data Privacy Governance Policy for more details.

Accepted and authorized by:

Date: 01.06.2023


Alexander Knauer
Jörg Kampmeyer
Dr. Uwe Krotzer