Company GUIDELINE

Marabu

Data Protection Policy of the Marabu Group

20/04/2018

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de ·www.marabu-druckfarben.de

Marabu

Contents

I. Preamble 3
II. Objective of the data protection policy 3
III. Scope and amendments to the policy 3
IV. Definitions 4
V. The Group Data Protection Officer 5
VI. Applicability of national law 7
VII. Requirements for the processing of personal data 7
VIII. Protection of the rights of data subjects 9
IX. Legitimacy of data processing 9
X. Transmission of personal data 18
XI. Contract data processing 22
XII. Rights of the data subject 23
XIII. Confidentiality of processing 25
XIV. Data and processing security 26
XV. Data protection monitoring and control 26
XVI. Data protection incidents 27
XVI. Responsibilities and sanctions 27
XVII. Entry into force and notification 29

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

I. Preamble

In the digital era we use modern means of communication daily, both in our internal processes and in our work with customers and suppliers. This generally involves the recording, processing and storage of data. Regardless of where this data is used, a high level of data protection and data security must always be ensured. This applies to data from customers, potential customers and other business partners just as it does to employee data. Because protecting data protects the person.

It is of the utmost priority to us that we ensure there is a uniform standard valid worldwide for the handling of personal data. For the protection of the personal rights and privacy of each individual provides us with the foundation for a business relationship based on trust.

Our corporate data protection policy meets the requirements of the European General Data Protection Regulation (hereafter GDPR) and ensures compliance with the principles of national and international data protection laws applicable worldwide.

Our executives and employees have a duty to comply with this corporate data protection policy and to uphold the respective data protection laws.

II. Objective of the data protection policy

This data protection policy creates one of the necessary basic conditions for the worldwide transfer of data between the group companies and ensures the adequate level of data protection required by the European GDPR and the national laws for the flow of data across international borders, including to those countries in which the laws provide no adequate level of data protection.

III. Scope and amendments to the policy

This data protection policy applies to all companies in the Marabu Group and their employees. The data protection policy applies to all processing of personal data.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

In countries in which the data of legal entities is protected in the same way as personal data, this data protection policy applies in the same way. Exception: Anonymised data, e.g. for statistical analyses or studies, is not subject to this data protection policy.

The individual group companies do not have the right to adopt rules which deviate from this data protection policy. Additional data protection policies may be drawn up in consultation with the Group Data Protection Officer (hereafter GDPO) if this is necessary under the respective national law. Any amendments to this data protection policy will be made in consultation with the GDPO within the procedure set out for the amendment of policies. The companies of the Marabu Group will be informed immediately of amendments within the procedure set out for the amendment of policies.

IV. Definitions

- The EU Commission considers the level of data protection in third countries to be adequate if the core privacy elements, according to the understanding agreed upon by the EU member states, are essentially protected. In making its decision, the EU Commission takes into account all of the circumstances that play a role in data transmission, or in a category of data transmission. This includes an assessment of the national law, as well as the code of professional conduct and security measures in place in each case.
- Data is **anonymised** when a connection to a person can no longer be made, or when a connection to a person can be restored only with a disproportionately large expense in terms of time, cost and labour.
- **Personal data particularly worthy of protection** is data which reveals the racial or ethnic origin, political views, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the clear identification of a natural person, and data concerning the health, sex life or sexual orientation of a natural person. On the basis of national law, further data categories can be classified as particularly worthy of protection or the content of data categories can be filled in differently. Equally, data

Marabu

relating to offences may only be processed under special conditions laid down by national law.

- The **data subject** within the meaning of this data protection policy is any natural person who is the subject of data being processed. In some countries, the data subject may also be a legal entity.
- **Data protection incidents** are all events where there is a reasonable suspicion that personal data has been illegally spied out, collected, changed, copied, transferred or used. These may concern actions by third parties and by employees.
- A **third party** is any person who in the view of the data controller is not directly involved. Contract data processors in the EU are not third parties within the meaning of data protection law because they report by law to the data controller.
- **Consent** is a voluntary, legally-binding declaration of consent to data processing.
- The processing of personal data is **necessary** if the valid purpose or legitimate interest could not be achieved without the personal data in question, or could be achieved only at a disproportionately high cost.
- **Personal data** is all information which relates to an identified or identifiable natural person. A person is identifiable for example if the connection to the person can be established by the information from the data combined with supplementary knowledge, even if such knowledge is available only by coincidence.
- **Transmission** is any disclosure of protected data to third parties by the data controller.
- The **processing of personal data** is any action, carried out with or without the assistance of automated processes, that serves to collect, save, organise, store, change, access, use, pass on, transmit, distribute, combine or compare data. This also includes the disposal, deletion and blocking of data and data storage media.
- The **data controller** is the legally independent entity within the Marabu Group that initiated the data processing measure in question through its business activities.

V. The Group Data Protection Officer

The GDPO is an internal body who does not take instructions in respect of data protection and works towards ensuring that national and international data protection laws are complied with. He is responsible for and monitors compliance

Marabu

with the data protection policy. The GDPO is appointed by the Management Board of the Marabu Group.

Any data subject can contact the Group Data Protection Officer with suggestions, queries, requests for information or complaints in connection with issues relating to data protection or data security. Queries and complaints will be treated confidentially if requested.

The decisions made by the GDPO concerning remedy for data protection breaches are to be taken into account by the respective management boards. Queries from supervisory authorities are always to be brought to the attention of the GDPO.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

VI. Applicability of national law

This data protection policy contains the data protection principles accepted worldwide, without replacing existing national law. The respective national law will have priority if it requires deviations from this data protection policy or places further requirements. The content of this data protection policy is to be complied with if there is no corresponding national law. The existing reporting obligations for data processing under national law have to be complied with.

Every company in the Marabu Group is responsible for compliance with this data protection policy and meeting their legal obligations. If it has reason to believe that the legal obligations conflict with the obligations under this data protection policy, the group company concerned has to inform the GDPO immediately. In the event of a conflict between national law and the data protection policy, the Marabu parent company will seek a practical solution together with the group company concerned in line with the objectives of the data protection policy.

VII. Requirements for the processing of personal data

1. Legitimacy

When processing personal data, the personal rights of the data subject have to be protected. Personal data has to be collected and processed in a legitimate manner (see also IX. Legitimacy of data processing).

2. Purpose

The personal data may only be processed for the purpose stated before the data was collected. Subsequent amendments to the purpose are only possible to a limited extent and require a justification and where applicable the approval of the data subject.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

3. Transparency

The data subject has to be informed in an adequately transparent manner of the processing of his data. Personal data will preferably be collected from the data subject himself.

4. Data minimisation

Before any personal data is processed, it has to be checked whether and to what degree this is necessary in order to achieve the purpose pursued with the processing. If it is possible to achieve the purpose and the cost is in proportion to the purpose pursed, anonymised or pseudonymised data is to be used.
Personal data may not be stored for potential future purposes unless required or allowed by national law.

5. Memory limitation

Personal data which is no longer needed after the expiry of statutory or business-process-related retention periods has to be deleted. If there is any evidence in an individual case of interests worthy of protection, the data has to be stored until there is legal clarity concerning the interest worthy of protection.

6. Data factually correct and up to date

Personal data must be correct, complete and up to date when stored. Suitable steps must be taken to ensure that incorrect, incomplete or outdated data is deleted, corrected, supplemented or updated.

7. Integrity and confidentiality

Personal data is to be treated as confidential. It has to be treated confidentially in personal dealings and protected with appropriate organisational and technical measures against unauthorised access, unlawful processing or disclosure, and accidental loss, alteration or destruction.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

VIII. Protection of the rights of data subjects

The GDPR grants data subjects a range of clearly defined rights. It therefore has to be ensured that queries from data subjects are processed in due time and correctly. As a rule, requests from data subjects are to be responded to immediately, and within one month at the latest. In exceptional cases the deadline may be extended by a further two months, e.g. due to complexity. The data subject has to be informed of the deadline extension with the reasons for the delay stated (see also XII. Rights of data subjects).

The rights of data subjects are the right to

- Information
- Correction
- Deletion
- Limitation of processing
- Data portability
- Not to be subjected to an automated individual decision
- Revocation of consent

IX. Legitimacy of data processing

The collection, processing and use of personal data is only allowed if one of the following circumstances for authorised data processing apply. Such a circumstance is also necessary if the purpose for the collection, processing and use of the personal data is to be amended compared to the original purpose.

IX.1. Customer and partner data

1.1 Data processing for a contractual or pre-contractual relationship

Personal data of potential customers, customers or partners concerned may be processed for the establishment, execution and termination of a contract. This also includes the support for the contract partner, provided that this is in connection with the purpose of the contract. Prior to a contract - contract initiation phase - the processing of personal data is allowed for the preparation of offers or to meet any other wishes of the potential customer aimed at the conclusion of a contract. Potential customers may be contacted during the contract initiation phase using the

Marabu

data they have provided. Any limitations expressed by the potential customers are to be observed.
If the data subject contacts a company in the Marabu Group with a request for information (e.g. request to be sent information about a product), the data processing is allowed in order to meet this request.

For advertising measures beyond this, the following requirements under 1.2 have to be met.

1.2 Data processing for advertising measures

Customer retention and advertising measures are subject to additional legal requirements. The processing of personal data for advertising, market/opinion research purposes is allowed if this is consistent with the purpose for which the data was originally
collected. The data subject is to be informed of the use of his data for advertising purposes and of his right to object.
If data is collected exclusively for advertising purposes, it is disclosed voluntarily by the data subject. The data subject should be informed that his disclosures for these purposes are made on a voluntary basis. In addition, the data subject should be advised of his right to object when he gives his consent to the processing of his data for advertising purposes.
The data subject should be able to choose for the purpose of giving consent between the available contact channels such as post, electronic post and telephone (Consent see 1.3).

If the data subject objects to the use of his data for advertising purposes, his data is no longer allowed to be used for these purposes and has to be blocked for these

Marabu

purposes. Additional restrictions in place in some countries concerning the use of data for advertising purposes are to be complied with.

1.3 Consent to data processing

Data can be processed if the data subject has given his consent. The declaration of consent has to be obtained in written or electronic form. In certain circumstances, e.g. during a telephone consultation, consent may be given verbally, in which case the consent must be documented. Any country-specific age limits for consent are to be observed.

1.4 Data processing permitted by law

The processing of personal data is also permitted if national legislation requests, requires or authorises this. The nature and scope of the data processing must be necessary for the data processing permitted by law, and must comply with the relevant statutory provisions.

1.5 Data processing to enforce a legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of the Marabu Group. Legitimate interests are usually of a legal nature (e.g. collecting outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed to enforce a legitimate interest if there is any evidence in an individual case that interests worthy of protection of the data subject outweigh the interest of processing the data. Before data is processed, it must be determined whether there are interests worthy of protection.

Marabu

1.6 Processing of data particularly worthy of protection

Personal data particularly worthy of protection may only be processed if this is required by law or the data subject has given his express consent. The processing of this data is also allowed if it is necessary in order to assert, exercise, or defend legal claims against the data subject. If the processing of data particularly worthy of protection is planned, the GDPO is to be informed in advance.

1.7 Automated individual decisions

Automated processing of personal data intended for the assessment of individual personality traits (e.g. creditworthiness) must not form the sole basis for decisions that have negative consequences or result in significant detriment to the data subject. The data subject must be informed of the fact that an automated individual decision-making procedure is carried out and of its result, and he must be given the opportunity to respond. In order to avoid incorrect decisions, it must be ensured that an examination and a plausibility check are carried out by an employee.

1.8 User data and internet

If personal data is collected, processed and used on websites or in apps, the data subjects are to be informed of this in data protection policies and where applicable in cookie policies. The data protection policies and where applicable cookie policies are to be integrated so that they are easily identifiable, directly accessible and constantly available for the data subjects.

If usage profiles are created to assess the usage behaviour of websites and apps (tracking), the data subjects have to be informed of this in each case in the data protection policy. Personal tracking can only take place if the national law permits this or the data subject has given his consent. If the tracking takes place under

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

a pseudonym, the data subject is to be given the opportunity to object (opt out) in the data protection policy.

If websites or apps allow access to personal data in an area requiring registration, the identification and authentication of the data subjects are to be arranged in such a way that adequate protection is achieved for the respective access.
If personal data is transferred via contact forms or via other areas on websites or apps requiring registration, it has to be ensured that the data transfer is encrypted to current standards.

IX.2. Employee data

2.1 Data processing for the employment relationship

In employment relationships, personal data may be processed if needed to establish, execute and terminate the employment agreement. During the application procedure, the personal data of applicants may be processed. If the candidate is rejected, his data has to be deleted in observance of the retention period requiring proof, unless the applicant has given his consent to the continued storage of his data for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other group companies.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data processing apply.

Marabu

If further information on an applicant needs to be collected a third party during the application procedure, the requirements of the respective national laws have to be observed. In case of doubt, consent must be obtained from the data subject.

If data needs to be processed in relation to the employment relationship but will not be used for the execution of the employment agreement, this has to be legitimised in each case by law. This legitimisation may be legal requirements, collective regulations with employee representatives, consent of the employee or the legitimate interest of the company.

2.2 Data processing permitted by law

The processing of personal employee data is also permitted if national legislation requests, requires or allows this. The nature and scope of the data processing must be necessary for the data processing permitted by law, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee worthy of protection must be taken into consideration.

2.3 Collective agreements for data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it is permissible if authorised by a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the respective employment law. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of national data protection law.

2.4 Consent to data processing

Employee data can be processed if the data subject has given his consent. Declarations of consent must be submitted voluntarily. Involuntary consent is void.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

The declaration of consent has to be obtained in written or electronic form. If the circumstances exceptionally do not allow this, the consent may be given verbally, in which case it must be properly documented. In the case of informed, voluntary disclosure of data by the data subject, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be informed in accordance with VI.3. of this data protection policy. The data subject can revoke his consent.

2.5 Data processing to enforce a legitimate interest

Personal employee data can also be processed if it is necessary to enforce a legitimate interest of the Marabu Group. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or commercial (e.g. valuation of companies) nature.

Personal data may not be processed to enforce a legitimate interest if there is any evidence in an individual case that interests worthy of protection of the employee outweigh the interest of processing the data. Before data is processed, it must be determined whether there are interests worthy of protection.

Control measures that require processing of employee data can only be implemented if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The legitimate interests of the company in the implementation of the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests worthy of protection that the employee affected by the measure may have in the exclusion of the measure and it can only be implemented if it is appropriate.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

The legitimate interest of the company and any interests of the employee worthy of protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

2.6 Processing of data particularly worthy of protection

Personal data particularly worthy of protection (see definition) may be processed only under certain conditions.

The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties in the area of employment law. The employee can voluntarily and expressly consent to the processing.

If the processing of data particularly worthy of protection is planned, the GDPO is to be informed in advance.

Marabu

2.7 Automated decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are assessed (e.g. as part of personnel selection or the assessment of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that there is a substantive assessment of the facts by a natural person, and that this assessment is the basis for the decision. The employee concerned must also be informed of the facts and results of automated individual decisions and given the opportunity to respond.

2.8 Telecommunications and internet

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related purposes. They are tools and a company resource. They can be used within the applicable legal regulations and internal company policies. If use is permitted for private purposes, the laws relating to secrecy of telecommunications and the respective national telecommunication laws must be observed insofar as these are applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the Marabu network that block technically harmful content or that analyse the attack patterns.
For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged temporarily. Person-related analyses of this data can only be conducted if there is a concrete justified suspicion that there has been a breach of laws or policies of the Marabu Group. These checks may only be conducted only by investigating departments while

Marabu

ensuring that the principle of reasonableness is observed. The respective national laws must be observed in the same manner as the existing group rules concerning this.

X. Transmission of personal data

Personal data may only be transmitted to recipients outside or inside the Marabu Group if the requirements under Section IX are met. The data recipient must be required to use the data only for the defined purposes.
In the event that data is transmitted to a recipient outside the Marabu Group to a third country, it must provide a data protection level equivalent to this data protection policy. If data is transmitted by a third party to a Marabu Group company, it must be ensured that the data may be used for the intended purpose.

In the event that a data subject claims that this data protection policy has been breached by the group company located in a third country that is importing the data, the group company that is exporting the data undertakes to support the data subject in establishing the facts of the matter and also asserting his rights under this data protection policy against the group company importing the data. In addition, the data subject is also entitled to assert his rights against the group company exporting the data. In the event of an alleged breach, the company exporting the data must provide the data subject with proof that the company importing the data in a third country has not committed any breach of this data protection policy in the further processing of the data received.

The GDPR allows data transmission to a third country in for example the following cases:

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

1. Adequacy of the data protection level in the third country determined by the Commission

The EU Commission can determine whether there is an adequate level of protection in a specific third country following an appropriate examination. The determination can also be limited to a specific region or a specific sector in the third country or to specific data categories. There is an adequate level of protection in the third country if, based on its national legislation and its application, the existence and effective operation of one or more independent supervisory authorities and the international commitments the third country has entered into, a level of protect exists which is equivalent to the level of protection granted in the GDPR. The GDPR provides for the continued validity of adequacy decisions already made. The Commission has already determined the adequacy of the data protection level for the "EU-US Privacy Shield".

2. Suitable guarantees provided

Data may be transmitted to a third country if the data controller or contract data processor has already provided suitable guarantees to ensure an adequate level of protection. The following guarantees come into consideration:

2. a Use of standard data protection clauses of the Commission or a supervisory authority

If the data exporter and data importer conclude a contract using the standard data protection clauses of the Commission, the data transfer is permitted by the supervisory authority without any further approval. If the standard data protection clauses are used in unaltered form, no approval is required for the data transmission.

Marabu

2. b Individually-negotiated contract clauses

Individually-negotiated contract clauses can also legitimise data transmission to a third country, but only after they have been approved by the responsible supervisory authority and the consistency mechanism of Art. 63. GDPR has been applied.

3. Exceptions for specific cases

Data may also be transmitted in a range of special cases stated explicitly and finally in the GDPR if no adequacy decision has been made by the Commission or there are no suitable guarantees. The circumstances for exceptions defined for this are to be interpreted narrowly in keeping with their exceptional nature.

3. a Consent

In order for the data subject's consent to the transmission of data to a third country to be effective, his express consent to disclose his data for the specific case is required. Furthermore, the potential risks of such data transmissions are to be made explicitly clear to the data subject, i.e. he should be informed in particular that the data protection level is not adequate and the rights of data subjects cannot be enforced. The data subject also has to be informed that he can revoke his consent at any time.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

3. b Necessary for performance of the contract

Data may be transmitted to a third country (subject to further requirements of the GDPO), if and to the extent which the transfer is necessary for the performance of a contract with the data subject or for the conclusion or performance of a contract on behalf of the data subject. Here it is in each case essential that this data transmission is strictly necessary for the performance of the contract.

3. c Pursuit of legal claims

The pursuit of legal claims can also legitimise data transmission if the data transmission is necessary for this purpose.

3. d Protection of vital interests

If the data subject is unable to give his consent for physical or legal reasons, the data may still be transmitted if this is necessary to protect his vital interests or the vital interests of other persons.

3. e Protection of compelling legitimate interests

Data transmission to a third country can be legitimised in an individual case if the data controller has a compelling legitimate interest in the transmission, data is not transmitted repeatedly, the data transmission concerns only a limited number of persons and is not precluded by overriding interests worthy of protection or rights and freedoms of the data subject and the data controller ensures the protection of personal data with suitable guarantees. The transmission may not already be based on another circumstance which allows data processing. If data is transmitted to a third country on this basis in an absolute individual case, both the supervisory authority and the data subject is to be informed of this.

Marabu

XI. Contract data processing

Contract data processing exists if a contractor is hired to process personal data, without being assigned responsibility for the related business process. In these cases, a contract data processing agreement is to be concluded with external contractors and between companies within the Marabu Group. The contracting company retains full responsibility for correct performance of the data processing. The contractor can process personal data only in accordance with the instructions issued by the client.

When placing the order, the following requirements must be complied with; the department placing the order must ensure that they are met.

1. The contractor must be chosen based on its ability to ensure the required technical and organisational protective measures.
2. The order is to be placed in writing an not exclusively by electronic means (e.g. transmission of personal data and selection of processing measures). The instructions on data processing and the responsibilities of the client and contractor are to be documented.
3. The contract standards provided by the GDPO are to be observed.
4. Before data processing begins, the client must be confident that the contractor will meet its obligations. A contractor can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.
5. In the case of contract data processing across international borders, the respective national requirements for disclosing personal data abroad must be met. In particular, personal data may only be processed in a third country only if the contractor can prove a level of data protection that is equivalent to this data protection policy.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

Suitable tools can be:

a. Agreement on EU standard contract clauses for contract data processing in third countries with the contractor and any subcontractors.

b. Participation of the contractor in a certification system recognised by the EU to create an adequate level of data protection.

c. Acknowledgement of binding company rules of the contractor to create an adequate level of data protection by the responsible data protection supervisory authorities.

XII. Rights of the data subject

Every data subject has the following rights. The assertion of these rights is to be processed immediately by the responsible unit and must not result in any disadvantage for the data subject.

1. The data subject may request information on which personal data is stored. If there are further rights in the employment relationship under the respective employment law to view the employer's documents (e.g. personnel file), these will remain unaffected.

   The data subject has to be informed of
   - the purpose of the processing
   - the categories of personal data
   - the recipients or categories of recipients, in particular in third countries
   - the planned length of time the data is to be kept, otherwise criteria for determining the length of time (e.g. term of contract)
   - the existence of the right to correct, delete, limit processing, object
   - the existence of a right to complain to a supervisory authority.

   In addition, further information has to be provided,
   - if personal data is not collected directly: the available information on the origin of the data
   - if an automated decision takes place: the meaningful information on the logic involved and the scope and implications for the data subject

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

- if a transmission to third countries takes place: information on the suitable guarantees.

2. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
3. The data subject can object to the processing of his data for advertising or market/opinion research purposes. The data must be blocked from these purposes.
4. The data subject has the right to request the deletion of his data if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests worthy of protection must be observed.
5. The data subject has a fundamental right to object to his data being processed, and this must be taken into account if the protection of his interests worthy of protection outweighs the interest of processing due to a particular personal situation. This does not apply if a legal regulation requires the data to be processed.

   If the data is used in direct marketing, in the event of an objection the processing for these purposes is prohibited and to be stopped immediately.
6. The data subject has the right to demand the "limitation of the processing" if the conditions below exist:
   - The correctness of the data is contested and the data controller has not yet been able to check this.
   - The processing is unlawful, but the data subject refuses the deletion of the data and instead demands a limitation.
   - The data controller no longer needs the personal data for the purposes of processing, but the data subject needs it to file, enforce or defend against legal claims.
7. The data subject who has provided the data controller with the personal data can demand from the data controller that it keeps this data in a structured, conventional and machine-readable format and transmits this data to another data controller without obstruction by the data controller (if technically feasible). This only applies if the processing is based on consent or a contract and is carried out with the aid of automated processes.

8. The data subject has the right not to be subjected to an automated decision which has a legal effect on him or similarly has a significant adverse effect on him (e.g. online credit application or online job application). Particular categories of personal data, e.g. data relating to health, may not be processed for the purpose of automated decisions, unless the data subject has expressly consented to this or a legal regulation requires this.

XIII. Confidentiality of processing

Personal data is to be treated as confidential. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing performed by an employee that he has not been tasked with as part of his duties and accordingly authorised to perform is unauthorised. The "need to know" principle applies. Employees may only have access to personal data if and to the extent which this is necessary for their respective duties. This requires the careful division and separation of roles and responsibilities, as well as their implementation and maintenance within authorisation concepts.

Employees may not use personal data for private or commercial purposes, or disclose it to or to make it available to unauthorised persons in any other way.

Supervisors must inform their employees at the start of the employment relationship of the obligation to maintain confidentiality. This obligation will continue after the employment relationship has come to an end.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

XIV. Data and processing security

Personal data must be is to be protected at all times against unauthorised access, unlawful processing or disclosure, as well as accidental loss, falsification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, in particular new IT systems, technical and organisational measures to protect personal data must be defined and implemented. These measures must take into account current standards of technology, the risks presented by the processing, and the need to protect the data (determined by the process for information classification). The technical and organisational measures for protecting personal data are part of the group-wide information security management system and have to be updated continuously to reflect technical developments and organisational changes.

XV. Data protection monitoring and control

Compliance with the data protection policy and the applicable data protection laws is monitored regularly with data protection audits and other controls. The performance of these controls is the responsibility of the GDPO or external auditors hired.
The Management Board of the Marabu Group is to be informed within the scope of the respective reporting duties of key findings.
Upon request, the results of data protection controls will be made available to the responsible data protection supervisory authority. The responsible data protection supervisory authority can perform its own controls within the limits of its authority under national law.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

XVI. Data protection incidents

All employees should inform their respective superior or the GDPO immediately of cases of breaches of this data protection policy or other regulations for the protection of personal data (data protection incidents).
The executive responsible for the function or the unit is required to inform the GDPO immediately of data protection incidents.
In cases of

- unintended or unlawful transmission of personal data to third parties,
- unintended or unlawful access by third parties to personal data, or
- loss of personal data

the required company reports (Information Security Incident Management) must be made immediately so that the reporting duties under national law can be met.

XVI. Responsibilities and sanctions

The management boards of the group companies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal data protection requirements and those contained in the data protection policy are met (e.g. national reporting duties).
It is the responsibility of executives to ensure with organisational, personnel and technical measures that data is processed properly taking into account data protection. Compliance with these requirements is the responsibility of the responsible employees. If data protection controls are performed by official agencies, the GDPO is to be informed immediately.

The respective management boards have to support the GDPO in his duties. The departments responsible for business processes and projects must inform the

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

Marabu

GDPO in good time about new processing of personal data. For data processing plans that may present particular risks to the personal rights of the data subjects, the GDPO is to be informed before processing begins. This applies in particular to personal data particularly worthy of protection. The executives must ensure that their employees are sufficiently trained in data protection.

Any improper processing of personal data or other breaches of data protection law is liable to prosecution in many countries and can result in claims for compensation. Offences for which individual employees are responsible can result in sanctions under employment law.

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de

XVII. Entry into force and notification

This policy will enter into force in this version upon its signing.
All employees of the Marabu Group will be notified of the policy by the executives.

The executives confirm receipt of the policy and accept its content with their signature.

Tamm, 26 April 2018

York Boeder	Rolf Simon	Dr. Mathias Ihme
CEO	MD	CIO DPO

Marabu GmbH & Co. KG · Tel.: +49-(0)7141-691-0 · info@marabu-druckfarben.de · www.marabu-druckfarben.de