DATA PROTECTION POLICY

MYTY

Inhalt

Version 1.0 vom 24.06.2025

1. Introduction

The personal data (hereinafter referred to as 'Data') processed by MYTY Group AG (hereinafter referred to as the 'Company') is of significant value to the Company and essential for its smooth operations. Therefore, such Data must be protected against risks in accordance with applicable laws, in particular the General Data Protection Regulation (hereinafter 'GDPR'). Furthermore, under Art. 25 GDPR in conjunction with Recital 78, the Company is obligated to implement an adequate strategy for protecting Data in its planned processing activities, taking into account the requirements specified therein. At the same time, the Company's customers, suppliers, employees, website visitors, and other business partners expect that the Data entrusted to the Company is subject to special protection and handled with the utmost care.

2. Objective

2.1. This corporate policy aims to establish uniform data protection standards across the company.

2.2. By adhering to the standards defined in this corporate policy, the company fulfills its data protection obligations and ensures appropriate consideration of the interests, fundamental rights, and freedoms of the data subjects.

2.3. Compliance with this corporate policy is a prerequisite for the secure exchange of personal data within the company and across the corporate group.

2.4. The introduction, implementation, and ongoing maintenance of this policy are intended to simultaneously demonstrate compliance with the requirements of the GDPR in accordance with Art. 5 (2) GDPR.

3. Scope

3.1. This corporate policy applies to any processing of personal data as defined by the GDPR, including the transfer of such data within the company. It regulates the data protection aspects that may arise in the context of data processing. The policy is applicable to all types of personal data, particularly data relating to employees, customers, suppliers, website visitors, and other business partners.

3.2. This internal data protection policy is mandatory and applies to all entities within the corporate group.

3.3. The origin and provenance of the data are not material to the applicability of this policy; the decisive factor is the processing of the data by the company.

4. Definitions

4.1. The definitions set out in Art. 4 GDPR shall apply.

5. Legal basis

5.1. For every data processing operation, it must be verified whether the intended processing of data is permissible and whether there is a legal basis for it, particularly in accordance with Art. 6 GDPR. If there are any doubts regarding the permissibility of the processing, the Data Protection Officer must be consulted.

5.2. As part of the permissibility assessment, it must also be examined whether the principles for the processing of personal data pursuant to Article 5 GDPR are complied with. This assessment must be documented for accountability purposes.

6. Principles

6.1. Lawfulness and transparency

6.1.1. When processing personal data, the principles of fairness and transparency must be observed.

6.1.2. As a general rule, the data subject must be informed when their personal data is being processed. The information provided must include all relevant details that are significant for the data subject and the exercise of their rights. Separate information may be omitted if the data subject is already aware of the data processing. This can be assumed, for example, if the data subject's consent has been obtained and they were informed about the processing in this context.

6.1.3. The information is provided through processing-specific privacy statements. These privacy statements are created and maintained by the Data Protection Officer.

6.2. Purpose limitation

6.2.1. Personal data may only be processed for the specific purpose for which they were originally collected. The purpose of data processing must always be lawful.

6.2.2. If personal data is to be processed for a purpose other than that for which it was originally collected, a compatibility assessment must be conducted to determine whether the new purpose is compatible with the original purpose.

6.3. Data Minimization

6.3.1. The company's data processing activities must be structured to minimize the processing of personal data. Default settings and options provided to data subjects must be designed to be privacy-by-default and privacy-by-design, in accordance with the principles of data protection.

6.3.2. When processing personal data, it must always be assessed whether the

intended purposes can be achieved by anonymizing or pseudonymizing the data. When implementing such measures, it is essential to ensure that the processed data no longer allows the recipient to identify individuals, or at least not without disproportionate effort.

6.4. Data accuracy and quality

6.4.1. All employees must ensure that personal data is accurate and kept up to date.

6.4.2. Inaccurate or incomplete personal data shall be rectified or erased. If a data subject requests rectification or completion, their legitimate request must be complied with without undue delay.

6.5. Storage limitation

6.5.1. When personal data are no longer necessary for the purposes for which they were collected or otherwise processed, they shall be deleted. For all personal data stored within the company, retention periods must be defined, taking into account any statutory retention obligations. Once the retention period or storage duration has expired, the data must be erased, preferably through an automated process.

6.6. Integrity and confidentiality

6.6.1. Ensuring data security is a top priority for the company. Data must be safeguarded against loss, unauthorized access, and other risks in accordance with applicable data protection regulations.

6.6.2. Appropriate measures must therefore be taken to ensure the protection of personal data. Protection shall be achieved through technical and organizational measures.

6.6.3. For each data processing operation, the specific protective measures implemented must be documented and regularly reviewed for their

appropriateness.

6.6.4. The IT department is authorized to issue further guidelines in the interest of data security, particularly regarding the use of IT systems within the company.

6.7. The concrete application of these principles is carried out in accordance with the regulations specified in Chapters 9 and following.

7. Lawfulness of processing based on legal obligations

7.1. The processing of personal data may be lawful, in particular, if it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

7.2. A lawful basis for data processing may also arise from a legal obligation of the company, which may result directly from a statutory provision or a binding regulatory decision.

7.3. The processing of personal data is also lawful if it is necessary for the establishment, exercise, or defence of legal claims in court. The same applies to the protection of vital interests.

7.4. Data processing is also permissible if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. The result of such a balancing of interests must be documented in writing.

8. Lawfulness of processing based on consent and documentation

8.1. The processing of personal data based on the data subject's consent is

permissible if the data subject has been sufficiently informed about the intended data processing in advance and has given their consent explicitly and on a voluntary basis.

8.2. Adequate information is provided when it is explained which data are processed and for what purposes. The data subject should be informed about the categories of recipients and that their consent is freely revocable. The process for revoking consent must be straightforward. Additionally, consent declarations must be clearly distinguishable from other declarations and must not be bundled with them. Separate consents should be obtained for different purposes.

8.3. Consent is only voluntary if the data subject is not disadvantaged by refusing or withdrawing it.

8.4. In any case, it must be ensured that there is clear affirmative action by the data subject. Consent declarations must be documented and retained for verification purposes in the event of subsequent review.

8.5. In cases where consent is given in writing, it may be permissible to scan the declaration and subsequently destroy the original document. If consent is obtained electronically, it must be ensured that a verification process is in place, such as a double opt-in procedure.

8.6. Requirements for consent may arise not only from the GDPR but also, for example, from the UWG (German Act Against Unfair Competition) or the TTDSG (German Telecommunications-Telemedia Data Protection Act). Further details can be found in Chapters 19 and following..

9. Communication and Procedures

9.1. If a request cannot be answered immediately or a claim cannot be fulfilled without delay, the data subject must at least be provided with interim

information indicating the expected processing time.

9.2. All requests must be communicated to the Data Protection Officer so that they can coordinate or take over further actions. Unless the Data Protection Officer explicitly assumes responsibility for processing the request, the respective department remains responsible for responding to the inquiry.

10. Right to information and access

10.1. Upon request, a data subject shall be informed whether the company processes personal data relating to them. If such processing takes place, the data subject has the right to obtain information about the personal data concerned. The data subject should specify the type of data for which they are seeking information.

10.2. Information shall be provided to the data subject in an intelligible form and language. When providing information, the personal data concerned and the purpose of storage must be communicated. Where available, the source of the data shall also be explained. Mandatory information includes any recipients of the data, the duration of storage, any automated decision-making, as well as references to the data subject's rights and the right to lodge a complaint with the supervisory authority.

10.3. When providing information in response to a data subject access request, the identity of the data subject must be verified. Additionally, it must be ensured that no personal data relating to third parties is disclosed in the process.

10.4. The provision of information is carried out in accordance with a defined process.

10.5. Further transparency obligations arise under Art. 19 GDPR following rectifications or erasures, and under Art. 26 GDPR in cases of joint controllership, which must also be fulfilled upon the data subject's request.

11. Right to rectification

11.1. Incomplete or inaccurate personal data shall be corrected upon request by the data subject. Ensuring such corrections is also in the interest of the company, as maintaining accurate and high-quality data records is essential.

11.2. If an employee becomes aware that personal data stored by the company is incomplete or inaccurate, the employee shall inform the relevant department so that the necessary corrections can be initiated.

12. Right to deletion and restriction

12.1. Upon a justified request by a data subject, the personal data stored about them shall be erased without undue delay. A request is considered justified in particular if there is no lawful basis for the processing of the data or if the lawful basis has ceased to exist. Even in the absence of a request by the data subject, personal data must be erased if there is no (longer any) lawful basis for their storage.

12.2. The data subject shall be informed within one month of receipt of the erasure request about the measures taken or, where applicable, the reasons for the refusal.

12.3. Where deletion is not feasible, it must be assessed whether at least a restriction of the processing of personal data can be implemented. In particular, processing should be restricted until the lawfulness of further data processing has been clarified. If the data subject no longer wishes their data to be used, restricting the processing should be considered to ensure that the data subject's data is not (re)used in the event of new data collection.

12.4. Complete erasure will not take place if statutory retention periods prevent deletion. In such cases, the data must be restricted from active use.

12.5. Further details are specified in the deletion concept.

13. Right to data portability

13.1. Data subjects also have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format. This right to data portability applies only to data processed based on consent, for the performance of a contract, or as part of automated processing.

13.2. When fulfilling the right to data portability, it is essential to verify the identity of the data subject. Additionally, care must be taken to ensure that no personal data of third parties is disclosed during the provision of information.

14. Right to object to processing

14.1. Where the processing of personal data is based on a relevant legal basis, the consent of the data subject is not required. If the data subject objects to the processing, it must be assessed to what extent the processing can be discontinued in the future. If this is not possible, the data subject must be informed accordingly.

15. Right to withdraw consent

15.1. Consent given by a data subject for the processing of their personal data may be withdrawn at any time. The data subject must be informed of the right to withdraw consent. The exercise of this right should be made as easy as possible. Withdrawal takes effect for the future. Data collected based on consent will be deleted upon withdrawal.

16. Data Protection Complaint

16.1. Data subjects have the right to lodge a complaint regarding the processing of their personal data within the company. Any complaint received must be promptly forwarded to the Data Protection Officer if it was not already addressed directly to them. The Data Protection Officer will respond to the complaint and, where necessary, propose appropriate measures to enhance the level of data protection.

17. Technical and organisational measures

17.1. The company implements appropriate technical and organizational measures, taking into account the nature, scope, context, and purposes of processing as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons. These measures are applied both at the time of determining the means for processing and at the time of the processing itself. The aim is to ensure and demonstrate compliance with this Regulation and to effectively implement data protection principles, such as data minimization.

17.2. The technical and organisational measures are designed to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services related to processing, in accordance with the principles of data protection.

17.3. Diese Maßnahmen werden regelmäßig, mindestens jedoch einmal jährlich durch den betrieblichen Datenschutzbeauftragten überprüft und aktualisiert.

17.4. Die technisch-organisatorischen Maßnahmen werden gegebenenfalls durch ein gesondertes Informationssicherheitsmanagementsystem nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ergänzt.

18. Record of Processing Activities

18.1. The company maintains a record of processing activities that involve the processing of personal data (Record of Processing Activities). This record is managed by the Data Protection Officer.

18.2. The introduction of new systems for the processing of personal data must be notified in advance to the Data Protection Officer. This ensures that the Data Protection Officer can assess the compliance of the processing with data protection regulations, update the record of processing activities, and adapt the privacy notices as necessary.

18.3. A risk assessment of the individual processing activities is an integral part of the documentation. Depending on the outcome of the risk assessment, a comprehensive Data Protection Impact Assessment (DPIA) must be prepared in addition to the standard documentation referred to in Section 4 of this chapter, involving the Data Protection Officer.

19. Notification of data breaches

19.1. Any personal data breach must, as a general rule, be reported to the competent data protection supervisory authority via the internal Data Protection Officer within 72 hours.

19.2. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the company shall also notify the affected data subjects without undue delay.

19.3. The business process to be followed in case of a personal data breach is defined by the notification procedure.

20. Data Protection Impact Assessment (DPIA)

20.1. If the intended processing of personal data is such that it corresponds to any of the processing operations listed in the 'mandatory list' of the data protection authorities, a DPIA must be conducted.

20.2. The same applies if the threshold assessment indicates that a DPIA must be conducted.

20.3. The DPIA is conducted by the company under the leadership of the internal Data Protection Officer.

21. Data Protection Officer as the point of contact

21.1. Appointment of a Corporate Data Protection Officer

21.1.1. The company has decided to appoint an external Data Protection Officer (DPO). The notification of this appointment has been submitted in accordance with the relevant data protection regulations.

21.1.2. "Prior to appointment, the company verified the professional suitability and any potential conflicts of interest.

21.2. Responsibilities and Powers of the Data Protection Officer (DPO)

21.2.1. The Data Protection Officer (DPO) coordinates the company's data protection activities. They serve as the primary point of contact for data subjects, employees involved in data processing, and the executive management.

21.2.2. The Data Protection Officer may, in the performance of their duties, address the executive management at any time and present their concerns.

21.2.3. Where necessary, the Data Protection Officer may issue supplementary guidelines or recommendations on specific topics in addition to this corporate

data protection policy.

21.2.4. The Data Protection Officer is authorized to monitor compliance with this corporate policy and the legal provisions of data protection law. Such monitoring may be conducted based on an audit plan agreed with the company management or on an ad-hoc basis. The corresponding supervisory authority does not relieve individual employees of their responsibility (LINK).

21.3. The tasks and responsibilities of the internal Data Protection Officer are set out in detail in this policy.

21.4. The above provisions shall apply mutatis mutandis in the event of the appointment of a Data Protection Officer for the United Kingdom ("UK DPO"). The process for notifying a UK DPO to the competent authority (Information Commissioner's Office, ICO) is described here. A tool to check any applicable fee obligations is available here.

22. Data Processing by a processor

22.1. When service providers perform services on behalf of the company, it must be assessed whether this involves the processing of personal data. This assessment is the responsibility of the relevant specialist department or the procuring unit. In case of uncertainties, the company's data protection officer must be involved.

22.2. If processors handle personal data on behalf of and under the instruction of the controller, it must be ensured that they are subject to the same duty of care as the controller itself.

22.3. Even when data processing is carried out by a service provider, the company remains the controller. Therefore, the service provider must be selected with due care.

22.4. No later than the commencement of the service provider's activities for the

company, it must be ensured that a separate data processing agreement in accordance with Art. 28 GDPR is concluded with the service provider. Thereafter, regular checks must be conducted to verify compliance with the obligations set out in the data processing agreement. Any deviations from the company's standard data processing agreement must be coordinated with the Data Protection Officer.

23. Joint Controllership

23.1. If, in the course of fulfilling their tasks, the company and the service provider jointly determine the purposes and means of the processing of personal data, they shall be considered joint controllers within the meaning of Art. 26 GDPR.

23.2. Joint controllership may also exist where the joint determination of the purposes and means of processing relates only to a part of the service and the associated data processing operations.

23.3. The responsibility for determining whether joint or sole controllership exists (on behalf of the company) and for selecting the appropriate contractual framework lies with the Data Protection Officer.

23.4. If joint controllership exists, it must be documented in accordance with a standard agreement. The agreement shall specify the responsibilities for each processing activity as well as the obligations regarding the safeguarding and fulfillment of data subjects' rights.

24. Marketing activities

24.1. Prior to the conclusion of a contract, it is permissible to process personal data during the contract initiation phase for the purpose of preparing quotes, drafting contract documents, and fulfilling other requests aimed at concluding a

contract.

24.2. Where prospective customers have given their consent, they may also be contacted using the data they have provided. Any restrictions specified by the prospective customer must be observed in this regard.

24.3. For the purpose of communication during an ongoing contractual relationship with a customer, the customer's consent for data processing is not required, provided that the processing is necessary for the performance of the contract. However, if the customer is to be contacted for marketing purposes during the contractual relationship, prior explicit consent must be obtained, preferably at the time the contract is concluded. This applies in particular to electronic communication.

24.4. Furthermore, the requirements of § 7 of the German Act Against Unfair Competition (UWG) must also be observed.

24.5. Sofern sich das Unternehmen bei der Vorbereitung und Durchführung von Werbemaßnahmen eines Dienstleisters bedient, werden die Aufgaben und Pflichten in einem entsprechenden Vertrag (z.B. Corporate Influencer, Social-Media-Monitoring, Webtracking, Affiliate etc.) niedergelegt. Sofern damit die Verarbeitung personenbezogener Daten einhergeht, ist zu prüfen, ob Verträge nach dem Abschnitt V abzuschließen sind. Daher sollte die Rechte und Pflichten bzw. die Weisungsgebundenheit in den Dienstleitungsverträgen möglichst genau beschrieben werden.

25. Cookies and similar technologies

25.1. The storage of information on a user's device or the access to information already stored on the device is only permissible if the user has given consent based on clear and comprehensive information.

25.2. This does not apply if the above-described processing is absolutely necessary

for the provider to make an explicitly requested telemedia service available to the user.

25.3. The fundamental requirement for consent entails the obligation to provide comprehensive information about the technologies used.

26. Processing of special categories of personal data

26.1. When processing personal data, it must be taken into account that special categories of personal data and data relating to particularly vulnerable data subjects may only be processed if additional conditions are met and/or specific safeguards are implemented.

26.2. Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. The processing of these special categories of personal data requires a specific legal basis in addition to the general conditions for lawful processing. Furthermore, appropriate technical and organizational measures must be implemented and documented to ensure a level of security appropriate to the risk.

26.3. Data relating to criminal convictions and offences shall not be processed. If, in the context of fraud prevention within the company, cases of suspected fraud are to be processed, this requires prior separate review and approval by the Data Protection Officer.

26.4. Additionally, it should be noted that minors are particularly vulnerable with regard to all personal data and therefore require special protection. Measures involving the processing of personal data must not be specifically targeted at

minors without prior review and approval by the Data Protection Officer.

26.5. Prior to the commencement of the aforementioned data processing, a Data Protection Impact Assessment (DPIA) must typically be carried out.

27. Transfer of personal data to third countries

27.1. The intended transfer of personal data to third countries requires a two-step assessment. At the first step, it must be verified whether there is a valid legal basis for such a transfer.

27.2. On the second level, it must additionally be assessed whether this transfer could adversely affect the interests and/or fundamental rights or freedoms of the data subject. In this regard, transfers to a contracting state of the European Union or the European Economic Area (EEA) are generally unproblematic. For all other countries, it must be verified in advance whether an adequate level of data protection exists. An adequate level can be achieved either through an adequacy decision by the European Union or by implementing additional contractual safeguards, such as the EU Standard Contractual Clauses (SCCs), potentially supplemented by further protective measures. If the recipient in the context of data transfers to the USA is not listed in the Data Privacy Framework (DPF), the adequacy decision cannot be relied upon in this case. Any transfer of personal data to a country outside the European Economic Area must be coordinated with the Data Protection Officer.

27.3. If the data transfer is based on the European Commission's Standard Contractual Clauses (SCCs), an additional Transfer Impact Assessment (TIA) must be conducted.

27.4. In the event that the company determines it is acting as a controller or processor not established in the European Union, it shall appoint a representative in the European Union (the 'EU Representative'). The same

applies if the company is established outside the United Kingdom and acts as a controller or processor; in such cases, the company shall appoint a representative in the United Kingdom (the 'UK Representative'). Service agreements shall be concluded with the EU Representative and/or the UK Representative, as applicable.

28. Employee Obligations

28.1. All employees of the company are explicitly obligated to maintain data confidentiality. They must be instructed that it is strictly prohibited to use personal data for private purposes, to disclose it to unauthorized persons, or to make it accessible to unauthorized parties. The obligation to maintain data confidentiality shall take effect at the start of employment with the company. Employees must also be informed that the duty of confidentiality extends beyond the termination of their employment with the company.

28.2. Within the company, it must be ensured that only employees who require access to personal data for the performance of their tasks are granted such access. This is regulated and enforced through an authorization concept.

28.3. All employees are obligated to support the Data Protection Officer in the performance of their duties and activities.

28.4. All employees are required to attend the company's internal data protection training at the beginning of their employment and subsequently on a regular basis. The responsibility for conducting these training sessions lies with the company's Data Protection Officer.

28.5. Any questions regarding this corporate data protection policy or the proper handling of personal data may be directed to the Data Protection Officer. The contact details of the Data Protection Officer are available in the Wiki.

29. Reporting of Breaches and Cooperation with Supervisory Authorities

29.1. Employees must immediately report to the Data Protection Officer if they become aware of any breach of this corporate policy or legal provisions relating to the protection of personal data.

29.2. Notification must be provided as soon as there are initial indications or suspicions of a data protection breach. This ensures that the Data Protection Officer is involved in clarifying the matter at an early stage. Further details regarding the procedure in the event of potential data protection breaches are outlined in a separate Data Breach Response Policy.

29.3. Based on the information received, the Data Protection Officer assesses whether there is an obligation to inform the supervisory authorities and the data subjects.

29.4. The company maintains a cooperative and trust-based relationship with the competent supervisory authorities. In the event of an obligation to provide information, the company will promptly furnish the requested details. Measures and findings of the supervisory authorities will be fully accepted by the company, provided they are lawful. All communication with the supervisory authorities shall be conducted through the Data Protection Officer.

29.5. The procedure for handling potential breaches is governed by a separate whistleblowing policy.

30. Internal Special Processes

30.1. The following special processes are governed by a separate IT policy:

- Clean Desk
- Bring Your Own Device

- Social Media Guideline
- Homeoffice policy

31. Responsibility

31.1. Primarily, employees entrusted with data processing are responsible for compliance with the provisions of this corporate policy.

31.2. All employees of the company are required to comply with this corporate policy and, by doing so, contribute to establishing and maintaining consistently high data protection standards across the entire organization.

31.3. Management is responsible for ensuring that all employees are informed about this corporate policy. This information must include the notice that violations of the provisions set out in this policy may result in criminal, liability, or employment law consequences.

31.4. The company remains the data controller within the meaning of data protection law vis-à-vis the data subject. Therefore, individual employees act on behalf of the company and must comply with its instructions and policies.

32. Public disclosure

32.1. This corporate policy must be made accessible to all employees of the company in an appropriate manner, particularly via the intranet.

32.2. This corporate policy is intended for internal use only and will not be publicly disclosed, as it constitutes an internal company guideline.

33. Amendments

33.1. The company reserves the right to amend this policy as necessary. Amendments may be required to comply with legal requirements, binding

regulations, requests from supervisory authorities, or internal company procedures. Employees will be informed of any changes to this policy through appropriate channels. It is their responsibility to familiarize themselves with the updated content.

33.2. Regular reviews shall also be conducted to assess whether technological changes necessitate adjustments to this corporate policy.