Premikati, Inc. Global Data Protection and Privacy Policy

1. Introduction

Premikati, Inc. ("Premikati"") is bound by data protection and privacy laws. Premikati respects and protects the rights of individuals, in particular the right to data protection and privacy during the processing and use of information as well as the right to privacy. The protection of information comprises the personal data of employees, applicants, customers, suppliers, partners, and all other persons within the Premikati area of responsibility. To adhere to this obligation, Premikati has adopted the Premikati Inc. Global Data Protection and Privacy Policy (Policy).

The Policy outlines a group-wide minimum standard for handling personal data in compliance with data protection and privacy laws. It defines requirements for all operational processes that affect personal data, as well as clear responsibilities and organizational structures. As soon as a process at Premikati involves collecting, processing, or using personal data, the provisions of this Policy are to be adhered to. Management of Premikati and the relevant process owners are responsible for ensuring that all processes – during which personal data is collected, processed, or used – are designed such that the provisions of this Policy are fulfilled. It is the duty of all Premikati employees to comply with the provisions of this Policy when handling personal data in their daily work for Premikati.

Premikati is headquartered in Indiana but does participate in the global economy. Therefore, the basic principles established through this Policy are based on the requirements of European data protection and privacy legislation. If, on a case-by-case basis, applicable local law outlines stricter data protection and privacy requirements than this Policy, personal data must be handled in compliance with those stricter laws. Additional standards and/or guidelines within the Premikati group that are issued as a result of this Policy must also take the applicable law into account in this respect.

This Policy shall not restrict the right of Premikati to use employee personal data to the fullest extent legally possible in order to preserve its position during any legal action or official proceedings. However, the applicable data protection and privacy law must be observed by Premikati, generally.

2. Definitions

Anonymized data Anonymous data	Data in a form that makes the direct or indirect identification of an individual person impossible, even with the aid of other data or information. Anonymous data does not have any reference to a person when it is collected. Anonymous and anonymized data is no longer subject to the internal or external data protection and privacy regulations.
Special categories of personal data	Contain data on the racial or ethnic origin, political views, religious or philosophical beliefs, union membership, felonies, penal convictions, health, or sexual preferences of persons, as well as data that can be misused for identity theft. For example, social security numbers, credit card and bank account numbers, as well as passport or driver's license numbers.

Person affected	An identified or identifiable natural person whose personal data is affected by a data processing action. A person is deemed identifiable if he or she can be identified directly or indirectly, in particular by reference to an identity number or to one or more factors specific to that person's physical, physiological, psychological, economic, cultural, or social identity.
Data processing actions (collecting, processing, and/or using)	Collecting means procuring data on the person affected. Processing describes any operation performed with or without the aid of an automatic procedure, or any set of operations connected with personal data, for example, collecting, saving, modifying, storing, changing, transferring, locking, or deleting personal data. Using means any usage of personal data, except for processing.
Third party	A natural or legal person, authority, institution, or any other office, except for the following: • The person affected; • The office responsible; • The commission data processor; • The persons who, under the direct responsibility of the data controller, are authorized to process the data
Consent	This may be explicit or implicit. Explicit consent generally requires an action by the person affected, through which they allow the processing of data – for example, the declaration of consent with the sending of e-mails or entering of personal data (opt-in). Explicit consent granted without duress is deemed to be the legal basis for the processing of personal data, provided no other legal provision is in force. Implicit consent (for example, opt-out) allows processing provided the person affected does not object.
Deletion	Either the physical destruction of data or the anonymization of data in such a way that makes it impossible to relate the data to a natural person.
Personal data	All information on an identified or identifiable natural person (person affected). A person is deemed identifiable if he or she can be directly or indirectly identified – in particular, by reference to an identity number or to one or more factors specific to that person's physical, physiological, psychological, economic, cultural, or social identity. For example, persons can be identified directly on the basis of names, telephone numbers, e-mail addresses, postal addresses, user IDs, tax numbers, or social security numbers, or indirectly on the basis

	of a combination of any information. Personal data that is subject to this Policy includes data on employees, applicants, former employees, customers, interested parties, suppliers, partners, users of Premikati web sites and services, and any other persons.
Premikati	Premikati and its 'affiliates' as defined by the German Stock Corporation Act (AktG), article 15 ff.
Data controller (controller)	A natural or legal person, authority, institution, or any other office that – either alone or in collaboration with others – makes decisions on the purposes and means of processing personal data (general legal definition). In the case of Premikati, Premikati is always the controller for the personal data of its employees, customers, suppliers, partners, or other persons. The controller is represented by the management legally responsible.

3. Basic Principles of Protecting Personal Data

During every process that includes collecting, processing, or using personal data, personal data may be processed or used only in accordance with this Policy and to the extent permitted by law.

Processing is only allowed in the following cases:

- If a person affected freely gave their consent, for example, when registering on a Web site
- If required to fulfill contracts with the person affected, for example, for an employment contract or a service contract
- If legally required or permitted, for example, due to tax or social security laws.

Personal data may be collected and processed for lawful purposes only. The respective purpose must be defined before the time at which the data is collected. Processing for a purpose other than the one defined before the data was collected is permitted in exceptional circumstances only if the person affected consents to the processing or if stipulated by law.

Personal data is to be collected directly from the person affected. Otherwise, the person affected must be at least informed of which types of personal data will be collected, processed, and/or used, and for which specific purposes.

Data may only ever be collected to the extent absolutely necessary for fulfilling the purpose specified before it is processed or used; any other processing is not permitted
.
Personal data must be accurate at all times and corrected where necessary.

Personal data may be retained only for as long as is absolutely necessary for the purposes specified or other legal requirements. Thereafter, personal data must be deleted or anonymized. For more information, see section 5b.

4. Responsibility for Data Protection and Privacy
   a. Management

   The legal responsibility for collecting, processing, and using personal data within Premikati lies with the executives of Premikati.

b. Internal Guidelines

Before commencing an activity during which access to personal data cannot be excluded, every employee and every third party acting on behalf of Premikati is to be instructed that they are not permitted to collect, process, or use personal data without authorization (data protection) and that this data must be handled confidentially (confidentiality).

Employees are to be made aware of the consequences of violating data protection and confidentiality. This Policy and other internal company guidelines that govern the handling of personal data are to be brought to employees' attention. The instruction must be documented in writing or in another form.

c. Employees

It is the duty of all Premikati employees to treat personal data to which they have access in the course of fulfilling their contractual duties with Premikati as confidential.

Premikati employees may collect, process, and/or use personal data only to the extent required to fulfill their duties and in accordance with approved processes. If collecting, processing, or using personal data is not recognizably prohibited for the employee, he or she can refer to the legality of the management's instructions.

5. Details

a. Notification, Accuracy of Data, and Inspection

A person affected must be informed in a suitable manner that their personal data is being collected, processed, and/or used. Usually, they are to be informed before the time at which data is collected.

The person affected must be informed by Premikati; the purpose for collecting, processing, or using the data, as well as other recipients to whom their data will be transferred. The information must be provided in a way that is easy to understand.

Stored personal data must be accurate. Inaccurate data must be corrected or deleted as soon as practicably possible. All processes for collecting, processing, and/or using personal data must contain an option for correcting, updating, and, where required by applicable law, deleting or blocking.

A person affected may, at any time, request information about the data stored on them, its origin, purpose for storing, and recipients to whom the data is passed on. Queries or complaints submitted by a person affected must be processed by Premikati without undue delay or according to those timeframes imposed by local law, whichever is the earlier. Objections from a person affected with regard to the processing of personal data must be investigated and, if necessary, remedial action must be taken.

b. Duration of Storage and Data Deletion

For every process in which personal data is collected, processed, or used, a schedule must be defined for the regular deletion of personal data after the specified purpose has been fulfilled or if the legal basis no longer applies.

Instead of deleting the personal data, it may also be irreversibly anonymized, meaning retained in such a way that makes it no longer possible to identify individual persons. If, for technical or legal reasons, it is not possible to either delete or anonymize personal data,

this personal data must be blocked for any further processing and/or use, as well as for further access.

c. Additional Rules for Special Types of Personal Data

Special types of personal data are details on racial and ethnic origin, political views, religious or philosophical beliefs, union membership, health, or sexual preferences. Special types of personal data are equal to such personal data that requires special sensitivity for the persons affected (sensitive data). For example, this is the case for data on criminal activities, as well as on those individuals who in their respective country fall below the age legally deemed as adult i.e., minors.

In the instances in which Premikati or third parties acting on behalf of Premikati collect special types of personal data, management must ensure that the persons affected have been informed in advance and have given their consent for this. Provided that applicable law does not determine otherwise, special types of personal data may be collected, stored, processed, and transferred only with the explicit consent of the persons affected. Increased precautions that are appropriate for the special sensitivity are to be taken for collecting, storing, processing, and transferring this data.

The following additional rules apply for these special categories of data:

- The collection, processing, and/or use of this data must be transparent for the persons affected at all times.
- Consent given by persons affected must refer explicitly to these special categories of data.
- Processes that involve collecting or using special types of personal data may be configured only with a prior check performed by Premikati's corporate counsel.

d. Transfer of Personal Data and Commissioned Data Processing

If personal data is to be exchanged within Premikati, it must first be checked whether contractual agreements on data protection and privacy, and data security are required. Such a check is always required if Premikati is to process data, or if an external service provider is to process data on behalf Premikati. A check is also necessary if Premikati transfers data to an external company, and the receiving company wishes to use the data for its own business purposes.

If personal data under the legal responsibility of Premikati is transferred to a recipient located outside the European Economic Area (EEA), it must also be ensured in advance that a suitable level of protection in accordance with Articles 25 and 26 of the EU Data Protection Directive (95/46/EC) is guaranteed.

If personal data is transferred, the following rules apply:

Transfer for commissioned processing:

If Premikati commissions or instructs an external company to collect, process, or store personal data is responsible for compliance with the requirements of data protection and privacy regulations. This responsibility does not cease with the transfer an external company.

Premikati must ensure that external companies that collect, process, or store personal data on their behalf, are reviewed in advance and then regularly to ensure that they comply with the

requirements of data protection and privacy regulations and that the necessary contracts with these companies have been concluded.

Transfer for recipient's own purposes:

The transfer of personal data to an external company for their own purposes is allowed only if this is permitted or required by law or if the persons affected have given their prior consent. Premikati must ensure that the legal requirements are checked before the data is transferred.

Transfer to state agencies (authorities and courts):
Premikati will transfer personal data to governmental agencies only on the basis of applicable law and after Premikati's corporate counsel have performed a prior check. In the event of a request for information from a governmental authority or a court of competent jurisdiction, Premikati will inform the person affected of this without undue delay.

6. Transfer of Customer Data
   Premikati processes customer personal data. This means not only the personal data pertaining to a customer's employees and business partners but also the personal data pertaining to the customers of Premikati customers. The transfer and use of such customer data must be performed in full compliance with applicable law and those additional obligations agreed in the contract between Premikati and the customer. Personal data of customers may never be passed on to third parties without an appropriate legal or contractual basis.

   In this respect, Premikati works with its customers to support them in complying with applicable data protection and privacy legislation; however, this does not include providing our customers with any legal advice or giving them any guarantee that their legal compliance with data protection and privacy laws are guaranteed.

7. Data Protection and Privacy Supervisory Authorities
   If so required by law, contract and/or the obligations set down in this Policy, Premikati must always cooperate with any data protection and privacy supervisory authority.

   If a data protection and privacy supervisory authority requests information or otherwise exercises their right of investigation, Premikati's corporate counsel must be informed without delay (chadbuchanan@premikati.com). The corporate counsel shall then act as the primary coordinator to formulate an appropriate response to the query. In addition, Premikati's corporate counsel will act as the direct contact with the respective data protection and privacy supervisory authorities.

8. Data Protection, Privacy, and Data Security
   Certain data protection and privacy laws require special security measures to be implemented when collecting, processing, and/or using personal data. Premikati shall define such measures in compliance with the legal requirements in the Premikati security policy and related security standards and guidelines. Premikati's corporate counsel shall assist in defining and updating these standards and guidelines.

9. Data Protection and Privacy Standards
   The requirements under this Policy can be specified and enhanced through data protection and privacy standards. Such data protection and privacy standards may only come into effect

after Premikati's corporate counsel has reviewed and approved their compatibility with this Policy.

10. Raising Awareness
    All employees and third parties acting on behalf of Premikati are regularly informed about both their duties and their rights within the scope of this Policy and applicable laws.