DATA PRIVACY AGREEMENT

Created by Kaduu AG

on 6th January 2023

1. RATIONALE AND PURPOSE
This Policy shall ensure that all Staff at all times comply with data protection requirements regarding the Processing of Personal Data.

2. APPLICABILITY
In case of Cross-Border Data Transfers, Personal Data may be subject to data protection laws and/or regulations of multiple jurisdictions. Hence, multiple local data protection policies may apply.

3 DEFINITIONS
Capitalized terms shall have the meaning assigned to them in this Policy. Applicable laws and/or regulations may contain different definitions, which shall be set out in the local data protection policies.

4 ROLES AND RESPONSIBILITIES

4.1 Global Data Protection Organisation and Framework
The Global Data Protection Organisation consists of the Global Data Protection Coordinator (GDPC), local Data Protection Officers (DPO) and local Data Protection Contacts (DPC).

The Global Data Protection Organisation maintains a Data Privacy Framework with several processes to support and advise Data Owners within CRO, COO, CFO and Business units with regard to their obligation to ensure and demonstrate compliance with data protection across global operations. These processes are set out in section 6 Processes.

4.2 Global Data Privacy Coordinator (GDPC)
The GDPC maintains the Global Data Protection Organisation and the processes under the Data Privacy Framework. The GDPC shall act as a point of contact for local DPOs/DPCs for inquiries related to data protection.

4.3 Data Protection Officer (DPO) and Data Protection Contacts (DPC)
Kaduu appoints a Data Protection Contact (DPC), or if required by applicable data protection law, a Data Protection Officer (DPO) as a member of the Global Data Privacy Organisation and a contact for the Data Privacy Framework.

The DPO/DPC implements and operates the Data Privacy Framework (in particular the processes set out in section 6 Processes) with regard to its Group Company. The DPO/DPC is responsible for monitoring and advising Kaduu with regard to its compliance with this Policy, the local data protection policy and applicable local data protection laws and/or regulations including the support of Staff with appropriate data protection trainings, awareness campaigns and documentations. .

4.4 Data Owner
The Data Owners are accountable that Personal Data in their area of responsibility is Processed in compliance with this Policy, the local data protection policy and applicable local data protection laws and/or regulations. Data Owners are supported by the Data Privacy Framework and the processes set out in section 6 Processes.

4.5 Competent CRO Function
The local Competent CRO Function provides advice regarding the interpretation of the applicable laws and/or regulations concerning data protection and, if applicable, banking secrecy or client confidentiality.

The local Competent CRO Function shall also be involved as early as possible in change initiatives involving new Cross-Border Transfers of Personal Data.

5. PRINCIPLES OF DATA PROCESSING

5.1 In General
Personal Data shall only be Processed by Kaduu in accordance with the principles set out in this section. If not indicated otherwise the principles apply to Kaduu both in its capacity as a Controller or a Processor of Personal Data.

It may be justified in specific cases to Process Personal Data contrary to such principles. However, any such exceptions must be based on applicable laws and/or regulations. In case of doubt about the lawfulness of the Processing the local DPC/DPO in collaboration with the responsible local Competent CRO Function needs to assess and confirm its legality.

Any exception to the principles must be requested by the Data Owner and be re- viewed by the local Competent CRO Function and the responsible DPO/DPC of Kaduu acting as Controller. The exception must be documented within the relevant Data Protection Impact Assessment (see section 6.2 Data Transfer Im- pact Assessment) or by way of another suitable means within the Data Privacy Framework.

5.2 Purpose
Subject to applicable laws and/or regulations, Personal Data may only be Processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes.

The purposes must relate to a relevant activity of a Group Company. All Staff is prohibited from Processing and disclosing any Personal Data obtained in their professional capacity for any private purposes.

The purpose for the collection and Processing of Personal Data must be notified to the Data Subject in accordance with section 5.6 Transparency and Notification. The change or extension of the purposes for Processing Personal Data is only permitted if covered by such notification or if required by applicable laws and/or regulations.

5.3 Need-to-Know Principle
The access to Personal Data must be limited to Staff which have a specific need to know for the relevant purposes as further specified in the Information Security Policy (see also section 5.5 Privacy by Design and Default).

5.4 Lawfulness, Fairness and Accuracy
Personal Data shall only be Processed lawfully and fairly (lawfulness and fairness).

Personal Data Processed must be accurate and, where necessary, kept up to date and complete. The Controller of Personal Data must take every reasonable step to ensure that inaccurate, outdated or incomplete Personal Data in view of the purpose of its collection is corrected and completed, or otherwise erased.

5.5 Privacy by Design and by Default
Taking into account in particular the international or commonly used standards and recommendations (such as ISO, EBDP), the cost, scope and purposes of Processing or Personal Data as well as the risks for the Data Subjects caused by the Processing, the Group Entity acting as Controller shall, both at the time of determining the means for Processing and during the Processing, implement appropriate technical and organisational measures, which are designed to implement data protection principles (such as pseudonymization, Data Minimization) and to integrate the necessary safe- guards into the Processing in order to meet the requirements of this Policy, local data protection policies and applicable data protection laws.

The Group Entity in its capacity as the Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data is Processed which is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimization).

This obligation relates to the amount of Personal Data collected, the extent of its Processing, the time period of its storage (see section 5.9 Data Retention and Erasure) and its accessibility (see section 5.3 Need-to-know).

5.6 Transparency and Notification
Personal Data shall be processed in a transparent manner.

To the extent required by local data protection laws, Kaduu as the Controller of Personal Data needs to provide Data Subjects with information on the Processing of their Personal Data (e.g. regarding the purposes of Processing, the legal grounds, information on cross-border transfers etc.). The content and process for such Notification are, if applicable, defined by the applicable data protection laws. The local data protection policies shall give further guidance.

5.7 Processing of Personal Data by Third Parties and/or Kaduu

If the Processing of Personal Data of a Company is carried out by Third Parties and/or Kaduu as Processor, such Processing shall be based on a data processing agreement. To the extent feasible, such data processing agreement Shall be based on the applicable templates as issued by the local DPO/DPC or Competent CRO Function. The DPO and shall approve global data processing agreements.

It must be ensured that the Personal Data is disclosed to such Third Parties and/or Kaduu in alignment with the principles set out in sections 5.3 and 5.5 above (Need-to-know and Privacy by Design and Default).

5.8 Cross-Border Data Transfers
The DPO/DPC of the transferring Company needs to assess new Cross-Border Data Transfers with a Data Privacy Impact Assessment and, if applicable, Data Transfer Impact Assessment (s. sections 6.2 Data Protection Impact Assessment and 6.3 Data Transfer Impact Assessment).

A Cross-Border Data Transfer from a country within the EU, EEA or from Switzerland is only allowed to countries with an adequate level of data protection or if allowed by applicable laws and/or regulations (which may include permission by contract establishing adequate data protection (e.g. EU SCC) or by consent of the respective Data Subject).

5.9 Data Retention and Erasure
Personal data shall not be retained for longer than required for the purpose for which is was collected or otherwise Processed, unless it is permitted or required by overriding applicable legal or regulatory obligations (e.g. archiving, tax, anti-money laundering), for the establishment, exercise or defence of legal claims or otherwise needed for overriding legitimate grounds (e.g. to comply with authority requests such as legal bans). The requirements regarding retention and archiving are set out a Archiving Policy for physical and electronic documents.

The ability to define and track retention periods and to erase personal data must be considered at the beginning of process planning or application implementation.

5.10 Consent of the Data Subject and other additional requirements
In certain jurisdictions, local laws and regulations define additional requirements with regard to the Processing of Personal Data (e.g. consent of a Data Subject regarding the Processing of Sensitive Data).

5.11 Processing of prospect client data
Depending on the jurisdiction in which Prospect Data is captured or retained, different rules may apply. Please refer to the Data capturing and retention during prospecting and local data protection policies for further guidance.

5.12 Information Security
Information Security defines the organisation and technical measures designed to ensure that Personal Data is adequately protected against unauthorized or unlawful Processing as well as accidental loss, destruction or damage in accordance with this Policy, local data protection policies and applicable data protection laws and regulations. Accordingly, all Staff and departments must adhere to the technical and organisational security policies and standards and applicable Security Controls and Standards thereunder.

6 PROCESSES

6.1 General
This Section 6 describes processes maintained by the Data Privacy Organisation to ensure and demonstrate compliance with data protection rules.

6.2 Data Protection Impact Assessments (DPIA)
To the extent required by applicable data protection laws, a DPIA needs to be carried out if anew Personal Data Processing activity is likely to result in a high risk to the rights and freedoms of data subjects, which must be determined in a risk assessment in collaboration with the competent DPO/DPC .Incase a high risk is likely, a DPIA has to be carried out by the

responsible for the new Personal Data Processing activity in collaboration with the competent DPO/DPC and risk mitigating measures may need to be implemented (full DPIA). If the risk level remains high despite the specified measures, the competent supervisory authority may have to be consulted in collabo- ration with the respective DPO/DPC before the data processing activity can start.

6.3 Data Transfer Impact Assessment (DTIA)
Cross-Border Data Transfers from the EU, EEA and Switzerland to a Third Party or to another Kaduu entity in a country without an adequate level of data protection may require the execution of a prior Data Transfer Impact Assessment (DTIA). The DTIA assesses the risks of foreign unlawful access and necessary contractual, organisational and/or technical safeguards for ensuring an adequate level of data protection.

Unless required by applicable data protection laws, the DTIA does not apply to Personal Data originating from Kaduu outside of the EU, EEA and Switzerland even if stored within the EU, EEA or Switzerland. Please contact your local DPO/DPC for further guidance.

6.4 Data Subject Requests
In some jurisdictions, Data Subjects may have certain rights with regard to the Processing of their Personal Data by Kaduu (Data Subject Requests). Such rights may include:

- The right to data access
- The right of rectification
- The right to erasure
- The right to restriction of processing
- The right to data portability
- The right to object

If applicable, the responsibilities and processes in case of Data Subject Requests shall be set out in the local Data Privacy Policy.

In some jurisdictions, Data Subject Requests must be answered within a short period of time. The Staff receiving a Data Subject Request must therefore forward such request immediately to the DPO/DPC in charge (incl. Data Subject Request Capture Forms, signed waiver and identity check as available on the internet). Depending on the nature of the request, the required steps are taken by the DPO/DPC (data sourcing and redacting, erasure of data, if applicable, etc.).

As set out in the applicable policies, all communications or requests for information on Personal Data (in particular client identifying information) from authorities are not handled via the Data Subject Request process but shall be forwarded immediately to the responsible Competent CRO Function.

6.5 Record of Processing Activities (ROPA)
If required by applicable law, each Controller and/or Processor within Kaduu shall maintain a Record of Processing Activities (ROPA) which shall contain the following information: (1) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (2) the purposes of the processing; (3) a description of the categories of data subjects and of the categories of personal data; (4) the categories of recipients to whom the personal data have been or will be disclosed including the categories of recipients in third countries or international organisations; (5) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case Suitable safeguards are required for data transfers by the applicable data protection laws, such safeguards; (6) where possible, the envisaged time limits for erasure of the different categories of data; (7) where possible, a general description of the technical and organisational security measures referred to in in the applicable data protection law.

The register for storing the Records of Processing Activities is centrally hosted by the GDPC and is maintained on a regular basis by the local DPO/DPC in charge.

Any new Processing activities which may have an effect on the content of the ROPA (e.g. new tools processing Personal Data) shall be reported to the local DPO/DPC in Charge as soon as possible.

6.6 Personal data breach

In some jurisdictions, a personal data breach needs to be notified to the competent supervisory authority if it is likely to result in a risk to the rights and freedoms of Data Subjects. If a data breach is likely to result in a high risk, data subjects may also need to be notified without undue delay. Any Staff confronted with a Personal Data breach must notify such breach via the Incident Management. The relevant DPO/DPC in charge will be notified and involved in accordance with the aforementioned process.

7 TRAININGS

To the extent required by the applicable laws and/or regulations Kaduu shall implement measures to raise awareness and offer trainings to their employees regarding their obligations under this Policy and the applicable data protection laws and/or regulation. The GDPC provides a high level training on data protection applicable to all Kaduu staff.