Contract data processing agreement in accordance with Art. 28 GDPR (General Data Protection Regulation)

annexed to the contract on the use of the LimeSurvey Professional online service

between

PagoPA

- Data controller, hereinafter referred to as the client -

and

LimeSurvey GmbH, Papenreye 63, 22453 Hamburg, Germany

-Contract administrator, hereinafter referred to as the contractor-

Preamble

This agreement clarifies and defines the data protection obligations of the contracting parties in the contractual relationship in accordance with Art. 28 GDPR, which result from the contract details applicable when using the LimeSurvey Professional online service offered, among other services, at www.limesurvey.org (General Terms and Conditions of the LimeSurvey Professional Online Service).

The contractor processes personal data for the client within the meaning of Art. 4 No. 2 and Art. 28 GDPR on the basis of this contract.

This agreement applies to all services provided by the contractor as part of the LimeSurvey Professional online service where employees of the contractor or their representatives may come into contact with the client's personal data.

§ 1 Object and duration of the contract, precedence

1. The object and duration of the contract are based on the performance agreements in the LimeSurvey Professional General Terms and Conditions.

2. The duration is based on the duration of the contract on the use of the LimeSurvey Professional online service, unless further obligations arise from the provisions of this Annex.

3. If this agreement deviates from other regulations made between the parties, the regulations of this 'Contract data processing agreement in accordance with Art. 28 GDPRGDPR (General Data Protection Regulation)' shall take precedence.

§ 2 Clarifying the contents

Type of data, processing type / purpose and categories of persons affected

1. Type of personal data (Art. 4 No. 1, 13, 14 and 15 GDPR)

Person master data
Person master data, like address, name, day of birth, etc.

Employment data
Employment data, like the job title, the employing company, etc.

Client data
Data relevant to the data subject as client

Communication data
Communication data like email address, telephone number etc.

2. Processing type and purpose (Art. 4 No. 2 GDPR):

The type and purpose for the processing of personal data is derived from the LimeSurvey Professional General Terms and Conditions. In particular, LimeSurvey software for the creation of online surveys shall be provided by the contractor for the client.

3. Categories of persons affected (Definition Art. 4 No. 1 GDPR)

The following categories of persons affected are covered by the processing:

- Survey offer users / survey participants
- Customers as survey creators

4. Processing within the EU/EEA or third countries providing an adequate level of protection

Any transfer of personal data to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 ff. GDPR are met.

The provision of the contractually agreed data processing takes place exclusively in Germany. However, data processing does not take place in third countries.

§ 3 Technical / organisational measures

1. The contractor has ensured and documented the implementation of the necessary technical and organisational measures. These can be seen in detail in Appendix 1. The client is aware of these technical and organisational measures and, in the assessment, the client agrees with the contractor that they provide an adequate level of protection for the associated level of risk.

2. The contractor thus ensures the provision of the security measures in accordance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in connection with Art. 5 para. 1 para. 2 GDPR. Overall, the measures to be taken concern data security measures which are there to ensure a level of protection that is appropriate for the associated level of risk with regard to the confidentiality, integrity, availability and resilience of the systems involved. The state of the technology implemented, the implementation costs and the type, scope and purposes of processing as well as the different occurrence probabilities and the severity of the risks to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR are taken into account.

3. The client undertakes to configure the software in accordance with data protection requirements when using the contractual services, in particular, to activate SSL encryption to protect the transmitted data.

4. Should the ownership or the confidentiality of the data controller be endangered through third-party measures (such as seizure), insolvency or settlement proceedings, or other events, the contractor must inform the data controller of this immediately.

5. If there is a risk of the client's data falling into the hands of third parties as a result of third-party measures (such as seizure), insolvency or settlement proceedings, or other events, the contractor is obliged to copy the data onto a suitable data carrier, to send this data carrier to the client as a backup and to delete the data on the data carrier affected by third-party measures or events. The data carrier stored until transfer must be specially marked up.

6. The technical and organisational measures are subject to general technical progress and further development. In this

respect, the contractor is permitted to implement alternative adequate measures. In such cases, the safety level of the defined measures shall not be compromised. As far as possible, personal data is to be transmitted and stored in encrypted form. The client will be given direct password-protected access to the respectively current version of the technical and organisational measures (Your Account).

7. If necessary, the contractor shall provide evidence to the client of the technical and organisational measures taken (see Appendix 1) within the framework of the client's control powers pursuant to § 7 of this contract.

§ 4 Rights of the data subjects; amendment, restriction of access and deletion of data

1. The contractor may not amend, delete or restrict the processing of the data processed as part of the contract on their own authority, such an action may only take place following the provision of documented instructions by the client. If an affected person contacts the contractor concerning this matter, the contractor shall immediately forward the request to the client.

2. The contractor shall support the client in the implementation of the rights of the data subjects and shall only act directly to the data subjects following the provision of documented instructions by the client.

When exercising support services under para. 2, the contractor is owed remuneration by the client

- if the contractor does not provide objective reasons for review by their own actions; or
- if the review takes the contractor more than one working day (8 hours) per contractual year; or
- if the client uses a LimeSurvey Professional service that is not billed on an annual basis.

Remuneration is calculated on a time-spent basis at EUR 120 net per commenced hour. The client shall bear the resulting additional costs incurred by the contractor.

§ 5 Other obligations of the contractor, in particular, quality assurance

The contractor undertakes to comply with the legal obligations in accordance with Articles 28 to 33 GDPR, in particular, however, to comply with the following requirements:

1. The contractor has appointed / appointed a data protection officer to carry out their activities in accordance with Articles 38 and 39 GDPR:

Mr.

Olaf Mangliers

Krohnskamp 35K

22301 Hamburg

Tel.: +49 40 43272727

wp@mangliers.de

Any change will be communicated to the client without delay.

2. Safeguarding confidentiality in accordance with Article 28 para. 3 p. 2 lit. b, 29, 32 para. 4 GDPR:

The contractor confirms that they are aware of the relevant data protection regulations for order processing; in carrying out the work, they shall only employ employees who are also bound to maintain confidentiality and data protection and who have previously been familiarised with the data protection regulations that are relevant to them. Any declarations of commitment must be prepared in such a way that they remain in force after the end of this contract or the employment relationship between the contractor and the persons they employ.

The contractor and any person under the authority of the contractor who has access to personal data may process such data exclusively in accordance with instructions provided by the client, including the powers granted in this contract, unless they are legally obliged to process such data (e.g. as a result of a request by investigative authorities for their surrender).

3. On request, both the client and the contractor shall cooperate with the supervisory authorities and provide assistance in the performance of their tasks.

4. The client shall be informed without delay of any control actions and measures taken by the supervisory authority in so far as they relate to this contract. This also applies if a competent authority conducts an investigation in the context of administrative or criminal proceedings with regard to the processing of personal data in the course of order processing with the contractor.

5. Insofar as the client, on their side, is subjected to an inspection by the supervisory authority, administrative or criminal proceedings, a liability claim of an affected person or a third party or any other claim in connection with the processing of the order with the contractor, the contractor must provide the best possible support. The contractor is to be remunerated by the client for carrying out support services. This is on a time-spent basis in the amount of EUR 120 net per commenced hour.

6. The contractor shall regularly monitor internal processes and technical and organisational measures to ensure that any data processing within their area of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the affected persons are protected.

7. The contractor must ensure that the technical and organisational measures taken can be proven to the client.

§ 6 Subcontracts / subcontractors

1. In principle the contractor may only assign subcontractors as further contractors with the prior written consent of the client. For this purpose, it is agreed that:

The client agrees to the assignment of the subcontractors specified in Appendix 2. The contractor shall also conclude agreements with these subcontractors in accordance with Art. 28 para. 2 to 4 GDPR and shall ensure contractually that the regulations agreed in this contract (particularly review and inspection rights of the data controller) also apply in principle against subcontractors.

The changing and replacement of subcontractors is permitted if there is a technical emergency and the continuation of data processing can only be secured by changing subcontractors. In this case, the change will be made and the client informed immediately.

Otherwise, the changing and replacement of subcontractors is permitted if:

- the contractor notifies the client of such replacements giving a reasonable period of notice, at the latest however, 2 weeks in advance of the data transfer, in writing or in text form (e.g. e-mail) and
- no objection has been raised by the client in writing or in text form up to the time of handover of the data to the subcontractor and
- a contractual agreement exists in accordance with Art. 28 para. 2 to 4 GDPR.
- if an objection is raised by the client, both parties shall endeavor to reach an agreement with regard to a solution. This may consist of the required corrective measures being taken by the subcontractor so that the subcontractor may be used or, failing this, the subcontractor can no longer be used. If no option is reasonable for the parties, both parties have the right to terminate the agreement within 30 days of efforts to find a solution failing.
- If an objection is not raised by the client, the subcontractor shall be deemed to have been approved by the client.

2. A transfer of the client's personal data is only permitted if the conditions specified in § 6 para. 1 are met.

3. If the subcontractor's services are provided outside the EU or the European Economic Area, the contractor is responsible for compliance with data protection measures.

4. Further outsourcing by the subcontractor requires the express consent of the prime contractor (written or text form in simple electronic format) as well as the immediate notification of the main client by the prime contractor. In this case, obligations contained in this agreement shall also be imposed on the other subcontractor.

§ 7 Client control rights

1. The contractor agrees that, within the framework of their control obligations in accordance with Art. 28 para. 3 lit. h GDPR, the client can monitor compliance with the provisions on data protection and in particular the contractual agreements, to an appropriate and necessary extent, in particular, by obtaining information in this regard and inspecting the stored data as well as the data processing programs used.

2. In order to exercise their statutory duty of control, the client may normally upon agreement of a date or advance notification during normal business hours and without disrupting the course of operations, ensure compliance with the provisions of data protection and in particular with this agreement to an appropriate and necessary extent at the contractor's premises via a person or several persons designated by him, such as a competent third party who is not in a competitive relationship with the contractor.

The contractor shall support the client during inspections and shall, in particular also, provide the client with any necessary information and evidence relating to the implementation of the technical and organisational measures.

For this purpose, the client may also have existing certificates from experts, certifications or assessments by the contractor submitted.

In the case of on-site reviews by the client, the contractor is owed remuneration in the amount of EUR 120 net per commenced hour. This shall not apply to cases where the contractor has given reasons to do so on the grounds of their own actions or omissions. Reviews up to a total of 8 hours per contractual year are exempt from the remuneration obligation under sentence 1. This exemption does not apply if the client uses a LimeSurvey Professional service that is not billed on an annual basis.GDPRGDPR

§ 8 Notification of data protection violations

1. The contractor shall inform the client immediately in the event of any serious disruptions to operations, suspicion of a personal data breach and measures relating to supervisory authorities or investigating authorities.

2. In the event of a personal data breach, the contractor shall take appropriate measures to safeguard data and to minimize any potentially disadvantageous consequences for the data subjects.

3. The contractor shall assist the client in compliance with the obligations referred to in Articles 32 to 36 of the GDPR with regard to the security of personal data, reporting obligations in the event of data leaks, data protection impact assessments and prior consultations with the supervisory authority. These include, among other things,

- ensuring an adequate level of protection via technical and organisational measures which take the circumstances and purposes of the data processing as well as the predicted probability and severity of a possible infringement of rights due to security vulnerabilities into account and enable the immediate identification of relevant infringement events
- reports concerning personal data breaches, which must be made to the client exclusively without delay
- fulfilling the obligation to assist the client in the context of their duty to inform the data subjects, if this cannot be carried out by the client themselves, and to make all information that is relevant in this regard available to the client without delay
- supporting the client in prior consultations with the supervisory authority, insofar as this is required and justified by law.

4. The client is obliged to inform the contractor immediately and comprehensively if they detect any errors or irregularities with regard to data protection regulations in the order results.

§ 9 Client's instructions

1. Instructions or directions from the client are to be addressed directly to the contractor using the contact details set out in para. 2. On the client side, the person authorised to access the login area at LimeSurvey.org, is deemed to be authorised to issue instructions.

2. Each party may specify/change the persons authorised to issue instructions by providing notification in a simple electronic format within the meaning of § 28 para. 9 GDPR (text form). The notification may be carried out

- via email to support@limesurvey.org or
- via the support centre at https://www.limesurvey.org/customer-support/contact-us

The amendment shall take effect upon immediate and explicit confirmation of the receipt of the declaration of the amendment by the other party.

3. The contractor is obliged to inform the client immediately if an instruction is liable to violate data protection regulations or the provisions of this contract. In this case, the contractor shall be entitled to suspend the execution of the respective instructions until they are confirmed or amended by the client.

4. The contractor agrees to not use the data provided for any purpose other than for the fulfilment of the contract.

§ 10 Deletion and return of personal data

1. Copies or duplicates of the data must not be created without the client's knowledge. Security backups, insofar as they are necessary to ensure proper data processing and legal retention periods are hereby unaffected.

2. After completion of the contractually agreed upon service provision or before, at the client's request - at the latest, however, upon termination of the service agreement - at the client's request, the contractor must hand over to the client, all documents, any generated processing and usage results as well as any data sets that exist in connection with the contractual relationship or destroy them in accordance with data protection regulations following receipt of prior consent.

3. In accordance with the respective retention periods, documentation that serves as proof of orderly and proper data processing must be kept by the contractor following completion of the contract. To assist the fulfilment of this obligation, these may be handed over to the client at the end of the contract.

§ 11 Liability

The client is solely responsible for the reliability of processing in accordance with Art. 6 para 2. GDPR and for safeguarding the rights of the data subjects. The client and the contractor shall be liable for damages to the data subjects in accordance with the provisions of Art. 82 GDPR. In accordance with Art. 82 para. 2 sentence 2 GDPR, the contractor is only liable for damages caused by processing if they have not complied with the obligations from the GDPR specifically imposed on them as a data processor, or if they have acted in breach of the legally issued instructions of those responsible for data processing or contravened these instructions.

A liability regulation agreed between the parties in the service contract (main contract for the provision of services) shall also apply to order processing, unless otherwise expressly agreed in this agreement.

§ 12 Final provisions

1. Amendments and changes to this Annex and the service agreement must be made

in writing or in text form in a simple electronic format within the meaning of Art. 28 para. 9 GDPR. This is also valid for any possible waiver of this requirement for written form.

2. Should any provision of this Annex or the service agreement be invalid or unenforceable, the validity of the other provisions shall remain unaffected. In such a case, the parties undertake to replace the invalid provision with another legally effective provision that fulfils the purpose of the provision being replaced.

3. With the conclusion of the present agreement on order processing, all possible previous agreements between the parties with regard to order (data) processing are cancelled.

4. The appendices are part of this Annex and are therefore also components of the performance contract:

- Appendix 1: Checklist of technical and organisational measures

- Appendix 2: Contractor's approved subcontractor list

_____, _____ Hamburg, 2020-06-24 19:19

_____ _____

PagoPA (Client contractor) Carsten Schmitz - CEO

Appendices

Appendix 1

Technical and organisational measures (TOM) checklist

In order to provide a guarantee for the lawful processing of personal data as part of the order to the contractor, the following technical and organisational measures in accordance with Art. 32 GDPR, shall be observed:

1. Confidentiality

a. **Access control** (e.g. for buildings and rooms, but also cabinets)

The minimum measures to prevent unauthorised access to data processing systems which are used to process personal data are:

Computer centre

- Electronic access control system with logging
- Guidelines for the monitoring and identification of guests in the building
- 24/7 Staffing of data centres
- Video monitoring of entries and exits

Office rooms (LimeSurvey GmbH)

- Visitors may not enter office premises without supervision.
- Access doors to office rooms should be particularly resistant and made of metal.
- All doors must be equipped with safety locks.
- Secure locking system using transponder cards
- Individually lockable cabinets

b. **Access control** (no unauthorised system use, e.g. unauthorised booting or unauthorised registration in systems)

Minimum measures to prevent the use of data processing systems by unauthorised persons are:

Computer centre

- The passwords for the supplied dedicated servers are changed by the client, LimeSurvey GmbH, after initial commissioning and are not known to the contractor (computer centre).

Software (LimeSurvey)

- Passwords in LimeSurvey are determined exclusively by the client.
- Passwords are not stored directly, only one Salted SHA-256 Hash is stored

Server system administration (LimeSurvey GmbH)

- Authentication using an asymmetric cryptosystem only (encryption via public and private keys)

Office rooms / employees (LimeSurvey GmbH)

- Authentication with the operating system and applications is carried out using an individual user ID and password
- Automatic barrier by screen saver with password input after 5 minutes of inactivity. The employees are also required to lock their workstations when leaving the room.
- Employees are required to keep passwords secret and to alter them if they suspect that passwords have been compromised.
- The following minimum requirements are imposed on the passwords:
- The password must have at least 10 characters.
    - The password must contain characters from at least three of the following four groups: a-z, A-Z, 0-9, other printable ASCII characters.
    - To reduce the risk that passwords can be guessed, trivial passwords may not be used (trivial meaning, e.g. a word from a dictionary, surname or first name, user ID, date of birth, vehicle registration number, telephone number or other information from the user's personal environment which may also be known to other persons).
- Employees are instructed to completely encrypt their computer hard disks, both for desktop PCs and for mobile PCs (notebooks, laptops).
- Employees are prohibited from using mobile data carriers or installing external software without prior agreement.

c. **Access contro** (running applications, preventing unauthorised activities in IT systems and accesses to data, applications and interfaces)

Minimum measures to ensure that those entitled to use a data processing system can only access the data covered by their access authorisation and that personal data cannot be unlawfully read, copied, modified or removed during processing:

System administration (LimeSurvey GmbH)

- Number of administrators reduced to those that are “essential”
- Full and proper deletion / destruction of data carriers before they are used for other purposes or passed on

- Administration of system and user rights by designated system administrators

Office rooms / employees (LimeSurvey GmbH)

- Number of administrators reduced to those that are “essential”
- The data processing systems (Internet, e-mail, server systems, etc...) are used exclusively for professional purposes.
- Content / data may only be stored on a server or on one's own PC if this is necessary for professional purposes. Content / data that is no longer required must be deleted.
- Regular checking and updating of authorisations including blocking access e.g. for retired employees
- Access logging and evaluation takes place at least once a year
- Verification and documentation of where personal data was transmitted (transmission control)
- Drive-specific access
- Full and proper deletion / destruction of data carriers before they are used for other purposes or passed on
- Use of document shredders that provide an appropriately high level of security
- A “Bring-Your-Own-Device” ban

d. **Separation control**

Minimum measures to ensure that personal data collected for different purposes and for different contracting entities is processed separately:

- Logical client separation (software-side)
- Establishment of individual database rights
- Separate database and database users with a password for each client
- Data collected with the contractual software will only be used by the client, or rather, for the purpose defined in the contract.

e. **Pseudonymisation**

As far as possible, the data will be processed in such a way that it can no longer be assigned to a natural person without the use of additional information.

LimeSurvey website

- The collection of IP addresses is avoided in system administration and any recorded IP addresses are made anonymous via shortening.

LimeSurvey SaaS

- Possibility of anonymisation / pseudonymisation by the client

2. Integrity

a. **Transfer control**

Minimum measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during

electronic transmission or during transport or storage on data carriers:

Data centre

- All employees have been instructed / trained in data protection.
- Deletion of data in accordance with data protection requirements after completion of the order.

Software (LimeSurvey)

- SSL connections always available (activated by default, can be activated/deactivated by the client at any time within the software)

Office rooms / employees (LimeSurvey GmbH)

- In principle, the use of mobile data carriers is prohibited.
- All employees are bound to secrecy in accordance with Art. 5 para. 2 GDPR.
- E-mail communication and access to LimeSurvey GmbH's employees' documents is protected by encryption and firewalls.
- Use of VPN's for mobile access to the company network

b. **Input control** (traceability, documentation)

Minimum measures to ensure that it is subsequently verifiable to determine who has access rights to enter, modify or remove personal data in data processing systems as well as being able to specify whether they have done so:

Software (LimeSurvey)

- Assignment of rights for the input, modification and deletion of data by the client
- Possibility of activating an audit log by the client to log data changes

Office rooms / employees (LimeSurvey GmbH)

- All employees sign a confidentiality clause, which also protects the client beyond their employment.
- All the contractor's employees may only access the data that is necessary for the completion of their work.
- Employees are only allowed to access customer data within the framework of clearly defined rules

3. Availability

Availability control

Minimum measures to ensure that personal data is protected against accidental destruction or loss, technical malfunctions caused by the failure of the operating / user software, negligent / intentional acts or damaging software:

Computer centre

- Use of interruption-free power supplies (USV)
- Devices for monitoring temperature and humidity in server rooms
- Fire and smoke detection systems
- The early fire detection system is connected to the fire alarm centre of the local fire department
- Air conditioning in server rooms

System administration (LimeSurvey Professional)

- Use of intrusion detection systems
- Use of anti-virus software
- Use of a software firewall
- Regular updating of all software components, at least every 7 days.
- Backup & recovery concept:
    - Generic data backup for all user files (images, design templates, etc.) which shall be backed up incrementally (i.e. changes only) every 24 hours.
    - A main backup is carried out every 7 days. A maximum of 2 main backups is provided.
    - The data in the user database is fully backed up every 24 hours. The last 7 days are stored for a day; weekly backups are kept for 4 weeks.
    - All data is encrypted during backup and stored on a special external data system (in the same data centre).
    - All servers are generally equipped with Raid 1 hard disk systems, in case of a hard disk failure the software continues to run on a hard disk after a short interruption in operation (restart of the server). As a rule, the defective hard disk is replaced within 24 hours, so that full security is ensured once again.

4. Control (other, review, assessment and evaluation)

Minimum measures to ensure that the measures are appropriate to ensure security and to withstand the loads, preferably at fixed minimum time intervals

In general,

- An external data protection officer is employed in accordance with the legal requirements.
- Employees are trained with regard to data protection

Data centre

- Data is stored separately from other data physically or logically.
- Data is also backed up on logically and/or physically separate systems.

LimeSurvey

- Logical client separation (software-side)
- Establishment of individual database rights
- Separate database and database users with a password for each client
- Data collected with the contractual software will only be used by the client, or rather, for the purpose defined in the contract.

Appendix 2: Contractor's approved subcontractor list

Subcontractor company	Address; country	Service
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen;Deutschland	Serverhosting (Bereitstellen der Hardware)