AGEM CORPORATE DATA PROTECTION POLICY

1. Purpose and objective

AGEM adopts this Policy in order to ensure basic and proportionate compliance with **Regulation (EU) 2016/679 (GDPR)** and, with respect to the group's Spanish reference legislation, Organic Law 3/2018 (LOPDGDD), regarding the processing of personal data of employees, candidates, customers, suppliers and other contacts related to its business activity.

Given that AGEM does not process special category data, nor carries out activities subject to specific privacy supervision, this Policy establishes only the minimum controls necessary to ensure adequate compliance without disproportionate administrative burdens.

This Policy is integrated into the Criminal Compliance System in accordance with UNE 19601, and is coordinated with the Code of Ethics, the Criminal Compliance Policy and the Ethics Channel Policy.

2. Scope of application

This Policy applies to:

- AGEM and all its subsidiaries and branches.
- All employees, executives and collaborators.
- Third parties who process personal data on behalf of AGEM (processors), by means of a contractual clause.

3. Roles and responsibilities

Sole Director

- Approves this Policy and ensures the minimum resources necessary for its implementation.
- Generally oversees compliance with legal obligations regarding privacy.

Compliance Officer

- Assumes the reference functions in data protection matters.
- Maintains the minimum compliance documentation (clauses, supplier contracts, basic activity record).
- Handles queries, incidents and requests to exercise rights.
- Coordinates the response to security breaches, should they occur.

Process owners

- Ensure that data within their area is processed lawfully, with minimisation and security.
- Ensure the use of forms and information clauses approved by the Compliance Officer.

4. Basic principles of processing

AGEM will proportionately apply the following principles:

4.1. Lawfulness, fairness and transparency

Data subjects will be informed, clearly and simply, of:

- the identity of the controller,
- the purpose of the data,
- the legal basis,
- any potential disclosures,
- the minimum retention period,
- the rights available.

These clauses will be included in employment contracts, contact forms, business relationships and any point of data collection.

4.2. Minimisation

Only the data strictly necessary to carry out AGEM's business and employment activity will be collected.

4.3. Accuracy

Data will be kept up to date where necessary (for example, employment, tax or contact data).

4.4. Storage limitation

Data will be retained only for:

- the duration of the contractual relationship, and
- the applicable legal limitation periods (employment, commercial or tax).

Once this period has elapsed, data will be deleted or kept blocked if there is a legal obligation to do so.

4.5. Security

AGEM will apply basic and proportionate technical and organisational measures:

- Strong passwords.
- User-based access control.
- Antivirus software and periodic updates.
- Backups.
- Restricted use of external devices and media.

Given the low risk of the data processed, advanced measures (full encryption, advanced anonymisation, etc.) are not required, unless the Compliance Officer determines otherwise.

5. Basic record of processing activities

AGEM will maintain, in simplified form, a **Record of Processing Activities (RoPA)** indicating, at a minimum:

- name of the processing activity,
- purpose,
- categories of data and data subjects,
- legal basis,
- retention periods,
- external processors, where applicable.

Data Protection Impact Assessments (DPIAs) will not be carried out unless a high-risk processing activity is introduced in the future.

6. Rights of individuals

AGEM guarantees the rights of access, rectification, erasure, objection, restriction and portability, in accordance with the GDPR.

The Compliance Officer will manage requests through the corporate privacy mailbox, verifying the requester's identity and responding within the maximum legal period.

7. Data processors

When a supplier has access to personal data (software, accounting firms, cloud services, maintenance), a data processing agreement will be formalised including:

- clear instructions,
- duty of confidentiality,

- proportionate security measures,
- obligation to notify incidents,
- return or deletion of data at the end of the service.

AGEM will select processors offering reasonable guarantees without the need for complex audits.

8. Security breaches

In the event of loss, unauthorised access or an incident affecting personal data:

- it will be reported immediately to the Compliance Officer,
- the severity will be assessed,
- the incident will be documented,
- the competent supervisory authority will be notified only if there is a risk to those affected (GDPR criteria),
- corrective measures will be communicated.

9. Minimum dissemination and training

AGEM will provide basic, brief privacy training to all staff, particularly in processes involving the management of personal data (administration, HR, sales).

An annual reminder will be sufficient given the low risk exposure.

10. Entry into force, review and update

The Policy will enter into force upon its approval by the Sole Director.

It will be reviewed every three years, or earlier if:

- AGEM's activities change,
- data processing activities change,
- there is a relevant regulatory update.

11. Compliance commitment

All staff must be aware of this Policy and comply with it.

Third parties with access to data will accept it through a contractual clause.

Annex I – AGEM Data Protection Operational Procedure

Simplified version, proportionate to risk

This Annex sets out the practical steps, minimum controls and responsibilities necessary to apply AGEM's Corporate Data Protection Policy. Its purpose is to ensure effective and proportionate compliance, avoiding unnecessary bureaucracy, in line with UNE 19601 and the actual risks of AGEM's activity.

1. Basic identification of processing activities (simplified RoPA)

The Compliance Officer will maintain a basic Record of Processing Activities, which will include only:

- Name of the processing activity (e.g. HR, customers, suppliers).
- Purpose.
- Legal basis (contract, legal obligation, legitimate interest, etc.).
- Minimum categories of data (identification, contact, billing, employment).
- Recipients (accounting firm, accounting software, cloud).
- Retention period.

Person responsible for each area: to inform the Compliance Officer when a new processing activity is created or an existing one is modified.

2. Data collection procedure and information clauses

Before collecting personal data from employees, candidates, customers, suppliers or any third party, the following must be ensured:

2.1. Mandatory use of brief information clauses

The area manager will provide/issue the corresponding information clause approved by the Compliance Officer.

Existing templates (mandatory use):

- Employment contract
- Recruitment process
- Customer forms
- Supplier forms
- Website contact forms

2.2. Minimum elements of the clause

All clauses must include:

- Identity of the controller (AGEM).
- Purpose of the processing.

- Legal basis (e.g. contract, legal obligation).
- Recipients.
- Retention period.
- Rights and the Compliance Officer's contact email.

3. Procedure for handling rights requests (access, rectification, erasure, objection, portability)

3.1. Enabled channel

All rights requests will be managed through a request email sent to the Compliance officer: dgomez@agemsa.com

3.2. Mandatory steps

- Register the request.
- Verify identity.
- Review with the relevant area whether the requested right applies.
- Respond within a maximum of 1 month.
- File evidence of the response.

3.3. Standard responses

The Compliance Officer will maintain response templates for:

- Access
- Rectification
- Erasure
- Objection
- Restriction
- Portability
- Inability to fulfil the right (reasoned)

4. Selection and management of suppliers with access to data (data processors)

4.1. Before contracting

The area proposing the supplier must verify with the Compliance Officer:

- Whether the supplier processes personal data on behalf of AGEM.
- Whether it offers reasonable security guarantees (declaration, basic certification, reputation).

4.2. Mandatory data processing agreement

A contract must be formalised with the legal minimum requirements:

- Process data only according to AGEM's instructions.
- Guarantee confidentiality.
- Adopt basic security measures.
- Notify incidents.
- Not subcontract without authorisation.
- Delete or return data at the end of the service.

The Compliance Officer keeps a copy of all contracts.

5. Minimum security measures applicable to AGEM

Given its activity and low risk level, AGEM applies basic technical and organisational measures:

5.1. Technical measures

- Devices protected with strong passwords.
- Automatic software updates.
- Active antivirus.
- Automatic backups.
- Data access limited to authorised profiles.

5.2. Organisational measures

- Prohibition on sharing passwords.
- Mandatory screen locking.
- Limited use of external devices.
- Responsible custody of paper documentation.
- Secure disposal of documentation.

5.3. Paperless whenever possible

Physical documentation will only be printed when strictly necessary.

6. Procedure for notification and management of security breaches

A security breach is any incident involving loss, theft, destruction or unauthorised access to personal data.

6.1. Immediate reporting

Every employee must immediately inform the Compliance Officer.

6.2. Internal steps

- Record the incident.
- Identify the affected data.
- Assess whether there is a risk to those affected.
- Adopt containment measures.
- Where applicable, notify the competent supervisory authority within 72 hours.
- Notify those affected if the risk is high.
- Document and close the incident.

7. Basic procedure for international transfers

AGEM will only carry out international transfers when:

- There is an adequacy decision, or
- Appropriate safeguards are in place (Standard Contractual Clauses), or
- It involves occasional technical support from European suppliers using certified infrastructure.

It is prohibited to engage suppliers outside the EEA without the Compliance Officer's validation.

8. Retention and deletion of data

Each area will comply with the following criteria:

8.1. Minimum retention

- Employment data: according to applicable regulations (4 to 10 years).
- Customer and supplier data: for the duration of the relationship plus applicable legal limitation periods.
- Non-contractual commercial data: maximum 2 years.

8.2. Deletion

Data will be deleted when no longer necessary, or kept blocked if there is a legal obligation to retain it.

9. Minimum training and awareness

The Compliance Officer will organise:

- Basic initial training for new hires.
- A brief annual reminder for all staff.
- Simple communications on good practices (email, brief document).

10. Periodic review of the Annex

The Compliance Officer will review this Annex every three years, unless legislative changes or new activities require otherwise.