HER BIOMEDICAL

POLÍTICA CORPORATIVA DE PROTECCIÓN DE DATOS DE AGEM

1. Objeto y finalidad

AGEM adopta la presente Política con el fin de garantizar el cumplimiento básico y proporcionado del Reglamento (UE) 2016/679 (RGPD) y de la Ley Orgánica 3/2018 (LOPDGDD), en relación con el tratamiento de datos personales de empleados, candidatos, clientes, proveedores y otros contactos vinculados a su actividad comercial.

Dado que AGEM **no trata datos de categorías especiales**, ni desarrolla actividades sujetas a supervisión específica en materia de privacidad, esta Política establece **únicamente los controles mínimos necesarios para asegurar un cumplimiento adecuado sin cargas administrativas desproporcionadas**.

Esta Política se integra en el Sistema de Compliance Penal conforme a la UNE 19601, y se coordina con el Código Ético, la Política de Compliance Penal y la Política del Canal Ético.

2. Ámbito de aplicación

Esta Política aplica a:

- AGEM y todas sus filiales y delegaciones.
- Todos los empleados, directivos y colaboradores.
- Terceros que traten datos personales por cuenta de AGEM (encargados), mediante cláusula contractual.

3. Roles y responsabilidades

Administrador Único

- Aprueba esta Política y garantiza los recursos mínimos necesarios para su aplicación.
- Supervisa, con carácter general, el cumplimiento de las obligaciones legales en materia de privacidad.

Compliance Officer

- Asume las funciones de referencia en materia de protección de datos.
- Mantiene la documentación mínima de cumplimiento (cláusulas, contratos con proveedores, registro de actividades básico).

- Atiende consultas, incidencias y solicitudes de ejercicio de derechos.
- Coordina la respuesta ante brechas de seguridad si se produjeran.

Responsables de proceso

- Garantizan que los datos de su área se tratan con licitud, minimización y seguridad.
- Aseguran la utilización de formularios y cláusulas informativas aprobados por el Compliance Officer.

4. Principios básicos de tratamiento

AGEM aplicará de forma proporcionada los siguientes principios:

4.1. Licitud, lealtad y transparencia

Los interesados serán informados, de forma clara y sencilla, de:

- identidad del responsable,
- finalidad de los datos,
- base jurídica,
- posibles comunicaciones,
- tiempo mínimo de conservación,
- derechos disponibles.

Estas cláusulas constarán en contratos laborales, formularios de contacto, relaciones comerciales y cualquier punto de recogida de datos.

4.2. Minimización

Solo se recabarán los datos estrictamente necesarios para desarrollar la actividad comercial y laboral de AGEM.

4.3. Exactitud

Se mantendrán los datos actualizados cuando sea necesario (por ejemplo, datos laborales, fiscales o de contacto).

4.4. Limitación de conservación

Los datos se conservarán únicamente durante:

- la vigencia de la relación contractual, y
- los plazos legales de prescripción aplicables (laborales, mercantiles o fiscales).

Finalizado ese periodo, serán eliminados o se mantendrán bloqueados si existe obligación legal.

4.5. Seguridad

AGEM aplicará medidas técnicas y organizativas básicas y proporcionadas:

- Contraseñas robustas.
- Control de accesos por usuario.
- Antivirus y actualizaciones periódicas.
- Copias de seguridad.
- Uso restringido de dispositivos y soportes externos.

Dado el bajo riesgo de los datos tratados, no se requieren medidas avanzadas (cifrado integral, anonimización avanzada, etc.), salvo criterio del Compliance Officer.

5. Registro básico de tratamientos

AGEM mantendrá, de forma simplificada, un **Registro de Actividades de Tratamiento (ROPA)** con indicación mínima de:

- nombre del tratamiento,
- finalidad,
- categorías de datos y de interesados,
- base jurídica,
- plazos de conservación,
- encargados externos cuando existan.

No se realizarán Evaluaciones de Impacto (DPIA/EIPD) salvo que se incorpore en el futuro un tratamiento de alto riesgo.

6. Derechos de las personas

AGEM garantiza los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad, conforme a lo previsto en el RGPD.

El Compliance Officer gestionará las solicitudes a través del correo corporativo destinado a privacidad, verificando la identidad del solicitante y respondiendo en el plazo máximo legal.

7. Encargados del tratamiento

Cuando un proveedor tenga acceso a datos personales (software, gestorías, servicios de nube, mantenimiento), se formalizará un **contrato de encargo de tratamiento** con:

- instrucciones claras,
- deber de confidencialidad,
- medidas proporcionales de seguridad,
- obligación de notificar incidentes,
- devolución o supresión de datos al finalizar el servicio.

AGEM seleccionará encargados que ofrezcan garantías razonables sin necesidad de auditorías complejas.

8. Brechas de seguridad

En caso de pérdida, acceso no autorizado o incidente que afecte a datos personales:

1. se comunicará inmediatamente al Compliance Officer,
2. se analizará la gravedad,
3. se documentará el incidente,
4. se notificará a la AEPD **solo si** existe riesgo para los afectados (criterio RGPD),
5. se comunicarán las medidas correctoras.

9. Difusión y formación mínima

AGEM impartirá una **formación básica y breve** en privacidad a todo el personal, especialmente en los procesos donde se gestionan datos personales (administración, RRHH, comercial).

El recordatorio anual será suficiente dada la baja exposición al riesgo.

10. Entrada en vigor, revisión y actualización

La Política entrará en vigor tras su aprobación por el Administrador Único. Será revisada de forma **trienal** o antes si:

- cambian las actividades de AGEM,
- cambian los tratamientos de datos,
- existe actualización normativa relevante.

11. Compromiso de cumplimiento

Todo el personal deberá conocer esta Política y ajustarse a ella. Los terceros con acceso a datos la aceptarán mediante cláusula contractual.

ANEXO I – PROCEDIMIENTO OPERATIVO DE PROTECCIÓN DE DATOS DE AGEM

Versión simplificada y proporcional al riesgo

Este Anexo establece los pasos prácticos, controles mínimos y responsabilidades necesarias para aplicar la Política Corporativa de Protección de Datos de AGEM. Su finalidad es asegurar un cumplimiento eficaz y proporcionado, evitando burocracia innecesaria, en coherencia con la UNE 19601 y con los riesgos reales de la actividad de AGEM.

1. Identificación básica de tratamientos (ROPA simplificado)

El Compliance Officer mantendrá un **Registro de Actividades de Tratamiento básico**, que incluirá únicamente:

1. Nombre del tratamiento (ej. RRHH, clientes, proveedores).
2. Finalidad.
3. Base jurídica (contrato, obligación legal, interés legítimo, etc.).
4. Categorías mínimas de datos (identificativos, contacto, facturación, laborales).
5. Destinatarios (gestoría, software contable, nube).
6. Plazo de conservación.

Responsable de cada área: informar al Compliance Officer cuando se cree un tratamiento nuevo o se modifique uno existente.

2. Procedimiento de recogida de datos y cláusulas informativas

Antes de recoger datos personales de empleados, candidatos, clientes, proveedores o cualquier tercero, debe asegurarse lo siguiente:

2.1. Uso obligatorio de cláusulas informativas breves

El responsable del área entregará/emitirá la cláusula informativa correspondiente aprobada por el Compliance Officer.

Modelos existentes (uso obligatorio):

- Contrato laboral
- Proceso de selección
- Formularios de clientes
- Formularios de proveedores
- Formularios de contacto web

2.2. Elementos mínimos de la cláusula

Todas las cláusulas deben incluir:

- Identidad del responsable (AGEM).
- Finalidad del tratamiento.
- Base jurídica (ej. contrato, obligación legal).
- Destinatarios.
- Plazo de conservación.
- Derechos y correo de contacto del Compliance Officer.

3. Procedimiento de atención de derechos (ARCO-P)

3.1. Canal habilitado

Todas las solicitudes de derechos se gestionarán a través de correo de petición realizado al responsable de Compliance: dgomez@agemsa.com

3.2. Pasos obligatorios

1. Registrar la solicitud.
2. Verificar identidad.
3. Revisar con el área correspondiente si procede el derecho solicitado.
4. Responder **en máximo 1 mes**.
5. Archivar evidencia de la respuesta.

3.3. Respuestas tipo

El Compliance Officer mantendrá modelos de respuestas para:

- Acceso
- Rectificación
- Supresión
- Oposición
- Limitación
- Portabilidad
- Imposibilidad de atender el derecho (motivado)

4. Selección y gestión de proveedores con acceso a datos (encargados del tratamiento)

4.1. Antes de contratar

El área que proponga el proveedor deberá verificar con el Compliance Officer:

- Si el proveedor **trata datos personales** por cuenta de AGEM.
- Si ofrece **garantías razonables** de seguridad (declaración, certificación básica, reputación).

4.2. Contrato obligatorio de encargo del tratamiento

Debe formalizarse un contrato con los mínimos legales:

- Tratar solo según instrucciones de AGEM.
- Garantizar confidencialidad.
- Adoptar medidas básicas de seguridad.
- Notificar incidentes.
- No subcontratar sin autorización.
- Eliminar o devolver datos al finalizar el servicio.

El Compliance Officer custodia una copia de todos los contratos.

5. Medidas mínimas de seguridad aplicables a AGEM

AGEM, dada su actividad y nivel de riesgo bajo, aplica medidas técnicas y organizativas básicas:

5.1. Medidas técnicas

- Equipos protegidos con contraseña fuerte.
- Actualizaciones automáticas de software.
- Antivirus activo.
- Copias de seguridad automáticas.
- Acceso a datos limitado a perfiles autorizados.

5.2. Medidas organizativas

- Prohibición de compartir contraseñas.
- Bloqueo de pantalla obligatorio.
- Uso limitado de dispositivos externos.
- Custodia responsable de documentación en papel.
- Eliminación segura de documentación.

5.3. Paperless siempre que sea posible

La documentación física solo se imprimirá si es estrictamente necesario.

6. Procedimiento de notificación y gestión de brechas de seguridad

Una brecha de seguridad es **cualquier incidente** de pérdida, robo, destrucción o acceso no autorizado a datos personales.

6.1. Comunicación inmediata

Todo empleado debe informar **de inmediato** al Compliance Officer.

6.2. Pasos internos

1. Registrar el incidente.
2. Identificar datos afectados.
3. Evaluar si existe riesgo para los afectados.
4. Adoptar medidas de contención.
5. Si procede, notificar a la AEPD **en 72 horas**.
6. Comunicar a los afectados si el riesgo es alto.
7. Documentar y cerrar el incidente.

7. Procedimiento básico para transferencias internacionales

AGEM solo realizará transferencias internacionales cuando:

- Exista decisión de adecuación, o
- Medidas adecuadas (Cláusulas Contractuales Tipo), o
- Se trate de soporte técnico puntual de proveedores europeos que utilicen infraestructuras certificadas.

Prohibido contratar proveedores fuera del EEE sin validación del Compliance Officer.

8. Conservación y eliminación de datos

Cada área respetará los siguientes criterios:

8.1. Conservación mínima

- Datos laborales: según normativa (4 a 10 años).
- Datos de clientes y proveedores: mientras dure la relación + prescripciones legales.
- Datos comerciales no contractuales: máximo 2 años.

8.2. Eliminación

Los datos se eliminarán cuando no sean necesarios o se bloquearán si existe obligación legal de conservación.

9. Formación y concienciación mínima

El Compliance Officer organizará:

- Formación básica inicial para nuevas incorporaciones.
- Un recordatorio anual breve para todo el personal.
- Comunicaciones simples sobre buenas prácticas (email, documento breve).

10. Revisión periódica del Anexo

El Compliance Officer revisará este Anexo cada **tres años**, salvo cambios legislativos o nuevas actividades que lo requieran.