POLÍTICA CORPORATIVA DE PROTEÇÃO DE DADOS DA AGEM

1. Objeto e finalidade

A AGEM adota a presente Política com o fim de garantir o cumprimento básico e proporcionado do **Regulamento (UE) 2016/679 (RGPD)** e, no que se refere à legislação espanhola de referência do grupo, da Lei Orgânica 3/2018 (LOPDGDD), no que respeita ao tratamento de dados pessoais de colaboradores, candidatos, clientes, fornecedores e outros contactos relacionados com a sua atividade comercial.

Dado que a AGEM não trata dados de categorias especiais, nem desenvolve atividades sujeitas a supervisão específica em matéria de privacidade, esta Política estabelece apenas os controlos mínimos necessários para assegurar um cumprimento adequado sem encargos administrativos desproporcionados.

Esta Política integra-se no Sistema de Compliance Penal em conformidade com a UNE 19601, e articula-se com o Código Ético, a Política de Compliance Penal e a Política do Canal Ético.

2. Âmbito de aplicação

Esta Política aplica-se a:

- AGEM e todas as suas filiais e delegações.
- Todos os colaboradores, diretores e colaboradores externos.
- Terceiros que tratem dados pessoais por conta da AGEM (subcontratantes), mediante cláusula contratual.

3. Papéis e responsabilidades

Administrador Único

- Aprova esta Política e garante os recursos mínimos necessários para a sua aplicação.
- Supervisiona, em termos gerais, o cumprimento das obrigações legais em matéria de privacidade.

Compliance Officer

- Assume as funções de referência em matéria de proteção de dados.
- Mantém a documentação mínima de cumprimento (cláusulas, contratos com fornecedores, registo de atividades básico).
- Atende consultas, incidências e pedidos de exercício de direitos.
- Coordena a resposta perante violações de segurança, caso ocorram.

Responsáveis de processo

- Garantem que os dados da sua área são tratados com licitude, minimização e segurança.
- Asseguram a utilização de formulários e cláusulas informativas aprovados pelo Compliance Officer.

4. Princípios básicos de tratamento

A AGEM aplicará de forma proporcionada os seguintes princípios:

4.1. Licitude, lealdade e transparência

Os titulares serão informados, de forma clara e simples, de:

- identidade do responsável,
- finalidade dos dados,
- fundamento jurídico,
- eventuais comunicações,
- prazo mínimo de conservação,
- direitos disponíveis.

Estas cláusulas constarão em contratos de trabalho, formulários de contacto, relações comerciais e qualquer ponto de recolha de dados.

4.2. Minimização

Apenas serão recolhidos os dados estritamente necessários para desenvolver a atividade comercial e laboral da AGEM.

4.3. Exatidão

Os dados serão mantidos atualizados quando necessário (por exemplo, dados laborais, fiscais ou de contacto).

4.4. Limitação de conservação

Os dados serão conservados apenas durante:

- a vigência da relação contratual, e
- os prazos legais de prescrição aplicáveis (laborais, mercantis ou fiscais).

Terminado esse período, serão eliminados ou mantidos bloqueados caso exista obrigação legal.

4.5. Segurança

A AGEM aplicará medidas técnicas e organizativas básicas e proporcionadas:

- Palavras-passe robustas.
- Controlo de acessos por utilizador.
- Antivírus e atualizações periódicas.
- Cópias de segurança.
- Uso restrito de dispositivos e suportes externos.

Dado o baixo risco dos dados tratados, não são exigidas medidas avançadas (cifragem integral, anonimização avançada, etc.), salvo critério do Compliance Officer.

5. Registo básico de tratamentos

A AGEM manterá, de forma simplificada, um **Registo de Atividades de Tratamento (RAT)** com indicação mínima de:

- nome do tratamento,
- finalidade,
- categorias de dados e de titulares,
- fundamento jurídico,
- prazos de conservação,
- subcontratantes externos, quando existam.

Não serão realizadas Avaliações de Impacto (DPIA/AIPD) salvo se, no futuro, se incorporar um tratamento de alto risco.

6. Direitos das pessoas

A AGEM garante os direitos de acesso, retificação, apagamento, oposição, limitação e portabilidade, em conformidade com o previsto no RGPD.

O Compliance Officer gerirá os pedidos através do correio corporativo destinado à privacidade, verificando a identidade do requerente e respondendo no prazo máximo legal.

7. Subcontratantes do tratamento

Quando um fornecedor tenha acesso a dados pessoais (software, gabinetes de contabilidade, serviços de nuvem, manutenção), será formalizado um contrato de subcontratação do tratamento com:

- instruções claras,
- dever de confidencialidade,

- medidas proporcionais de segurança,
- obrigação de notificar incidentes,
- devolução ou eliminação de dados no final do serviço.

A AGEM selecionará subcontratantes que ofereçam garantias razoáveis sem necessidade de auditorias complexas.

8. Violações de segurança

Em caso de perda, acesso não autorizado ou incidente que afete dados pessoais:

- será comunicado imediatamente ao Compliance Officer,
- será analisada a gravidade,
- o incidente será documentado,
- será notificado à autoridade de controlo competente apenas se existir risco para os titulares (critério RGPD),
- serão comunicadas as medidas corretivas.

9. Divulgação e formação mínima

A AGEM ministrará uma formação básica e breve em privacidade a todo o pessoal, especialmente nos processos onde se gerem dados pessoais (administração, RH, comercial).

O lembrete anual será suficiente dada a baixa exposição ao risco.

10. Entrada em vigor, revisão e atualização

A Política entrará em vigor após a sua aprovação pelo Administrador Único.

Será revista trienalmente ou antes se:

- mudarem as atividades da AGEM,
- mudarem os tratamentos de dados,
- existir atualização normativa relevante.

11. Compromisso de cumprimento

Todo o pessoal deverá conhecer esta Política e ajustar-se a ela.

Os terceiros com acesso a dados aceitá-la-ão mediante cláusula contratual.

Anexo I – Procedimento Operativo de Proteção de Dados da AGEM

Versão simplificada e proporcional ao risco

Este Anexo estabelece os passos práticos, controlos mínimos e responsabilidades necessárias para aplicar a Política Corporativa de Proteção de Dados da AGEM. A sua finalidade é assegurar um cumprimento eficaz e proporcionado, evitando burocracia desnecessária, em coerência com a UNE 19601 e com os riscos reais da atividade da AGEM.

1. Identificação básica de tratamentos (RAT simplificado)

O Compliance Officer manterá um Registo de Atividades de Tratamento básico, que incluirá apenas:

- Nome do tratamento (ex.: RH, clientes, fornecedores).
- Finalidade.
- Fundamento jurídico (contrato, obrigação legal, interesse legítimo, etc.).
- Categorias mínimas de dados (identificativos, contacto, faturação, laborais).
- Destinatários (gabinete de contabilidade, software de contabilidade, nuvem).
- Prazo de conservação.

Responsável de cada área: informar o Compliance Officer sempre que se crie um novo tratamento ou se modifique um existente.

2. Procedimento de recolha de dados e cláusulas informativas

Antes de recolher dados pessoais de colaboradores, candidatos, clientes, fornecedores ou qualquer terceiro, deve assegurar-se o seguinte:

2.1. Uso obrigatório de cláusulas informativas breves

O responsável da área entregará/emitirá a cláusula informativa correspondente aprovada pelo Compliance Officer.

Modelos existentes (uso obrigatório):

- Contrato de trabalho
- Processo de seleção
- Formulários de clientes
- Formulários de fornecedores
- Formulários de contacto no sítio Web

2.2. Elementos mínimos da cláusula

Todas as cláusulas devem incluir:

- Identidade do responsável (AGEM).
- Finalidade do tratamento.
- Fundamento jurídico (ex.: contrato, obrigação legal).
- Destinatários.
- Prazo de conservação.
- Direitos e correio de contacto do Compliance Officer.

3. Procedimento de atendimento de direitos (Acesso-Retificação-Apagamento-Oposição-Portabilidade)

3.1. Canal habilitado

Todos os pedidos de direitos serão geridos através de correio de pedido dirigido ao responsável de Compliance: dgomez@agemsa.com

3.2. Passos obrigatórios

- Registar o pedido.
- Verificar a identidade.
- Rever com a área correspondente se procede o direito solicitado.
- Responder no máximo em 1 mês.
- Arquivar evidência da resposta.

3.3. Respostas-tipo

O Compliance Officer manterá modelos de resposta para:

- Acesso
- Retificação
- Apagamento
- Oposição
- Limitação
- Portabilidade
- Impossibilidade de atender ao direito (fundamentada)

4. Seleção e gestão de fornecedores com acesso a dados (subcontratantes do tratamento)

4.1. Antes de contratar

A área que propuser o fornecedor deverá verificar com o Compliance Officer:

- Se o fornecedor trata dados pessoais por conta da AGEM.
- Se oferece garantias razoáveis de segurança (declaração, certificação básica, reputação).

4.2. Contrato obrigatório de subcontratação do tratamento

Deve formalizar-se um contrato com os mínimos legais:

- Tratar apenas segundo instruções da AGEM.
- Garantir confidencialidade.
- Adotar medidas básicas de segurança.
- Notificar incidentes.
- Não subcontratar sem autorização.
- Eliminar ou devolver dados no final do serviço.

O Compliance Officer conserva uma cópia de todos os contratos.

5. Medidas mínimas de segurança aplicáveis à AGEM

A AGEM, dada a sua atividade e nível de risco baixo, aplica medidas técnicas e organizativas básicas:

5.1. Medidas técnicas

- Equipamentos protegidos com palavra-passe forte.
- Atualizações automáticas de software.
- Antivírus ativo.
- Cópias de segurança automáticas.
- Acesso a dados limitado a perfis autorizados.

5.2. Medidas organizativas

- Proibição de partilhar palavras-passe.
- Bloqueio de ecrã obrigatório.
- Uso limitado de dispositivos externos.
- Custódia responsável de documentação em papel.
- Eliminação segura de documentação.

5.3. Paperless sempre que possível

A documentação física só será impressa se for estritamente necessário.

6. Procedimento de notificação e gestão de violações de segurança

Uma violação de segurança é qualquer incidente de perda, roubo, destruição ou acesso não autorizado a dados pessoais.

6.1. Comunicação imediata

Todo o colaborador deve informar de imediato o Compliance Officer.

6.2. Passos internos

- Registar o incidente.
- Identificar os dados afetados.
- Avaliar se existe risco para os titulares.
- Adotar medidas de contenção.
- Se aplicável, notificar a autoridade de controlo competente em 72 horas.
- Comunicar aos titulares se o risco for elevado.
- Documentar e encerrar o incidente.

7. Procedimento básico para transferências internacionais

A AGEM apenas realizará transferências internacionais quando:

- Exista decisão de adequação, ou
- Existam medidas adequadas (Cláusulas Contratuais-Tipo), ou
- Se trate de suporte técnico pontual de fornecedores europeus que utilizem infraestruturas certificadas.

Fica proibida a contratação de fornecedores fora do EEE sem validação do Compliance Officer.

8. Conservação e eliminação de dados

Cada área respeitará os seguintes critérios:

8.1. Conservação mínima

- Dados laborais: de acordo com a normativa (4 a 10 anos).
- Dados de clientes e fornecedores: enquanto durar a relação + prazos legais de prescrição.
- Dados comerciais não contratuais: máximo 2 anos.

8.2. Eliminação

Os dados serão eliminados quando deixem de ser necessários ou serão mantidos bloqueados caso exista obrigação legal de conservação.

9. Formação e sensibilização mínima

O Compliance Officer organizará:

- Formação básica inicial para novas admissões.
- Um lembrete anual breve para todo o pessoal.
- Comunicações simples sobre boas práticas (e-mail, documento breve).

10. Revisão periódica do Anexo

O Compliance Officer revisará este Anexo a cada três anos, salvo alterações legislativas ou novas atividades que o exijam.