REGULAMENTO INTERNO DE PROTEÇÃO DE DADOS PESSOAIS

O respeito pela privacidade dos titulares de dados pessoais que tratamos, é uma responsabilidade comum de todos quantos exercem funções no **Monte – Desenvolvimento Alentejo Central, ACE,** doravante designada por **MONTE**, estando orientado para a prossecução da total conformidade e cumprimento das regras e princípios do Regulamento Geral de Proteção de Dados (RGPD), aprovado pelo Regulamento (EU) 2016/679, de 27 de abril de 2016 e demais legislação aplicável, nomeadamente a Lei de Execução Nacional nº. 58/2019 de 8 de agosto. Tem ainda presente o disposto na Carta dos direitos fundamentais da União Europeia constantes do Regulamento (2016/C 202/02) de 7 de junho de 2016, a Resolução do Conselho de Ministros n.º 41/2018 que aprova a Estratégia Nacional de Segurança do Ciberespaço e o Decreto-lei n.º 65/2021 de 30 de julho, Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

1. ÂMBITO DE APLICAÇÃO

Este Regulamento deve ser integralmente cumprido e respeitado, por todos aqueles que tratam dados pessoais sob responsabilidade do **MONTE**, sem exceção, sendo obrigatórias para:

a) Todos os trabalhadores com vínculo laboral;

b) Dirigentes e membros dos órgãos sociais;

c) Técnicos, consultores e prestadores de serviços;

d) Estagiários e voluntários;

e) Qualquer pessoa que, no exercício de funções no Monte, tenha acesso a dados pessoais.

O presente Regulamento aplica-se a todos os tratamentos de dados pessoais efetuados pelo Monte, independentemente do suporte (físico ou digital). Abrange toda a metodologia de trabalho e processos, bem como materiais ou hardware (servidores, portáteis, discos duros, equipamentos nómadas, programas ou software, canais de comunicação (fibra ótica, wi-fi, Internet e Intranet), suportes em papel (documentos, fotocópias, microfilmes, etc.), bem como a sensibilização e a formação para a defesa da privacidade dos dados pessoais que tratamos.

2. OBJETIVO

Este Regulamento é um dos pilares do nosso objetivo para a conformidade com o RGPD, que entrou em vigor na União Europeia em 25 de maio de 2018, bem como das futuras certificações que o **MONTE** se proponha alcançar.

3. CONCEITOS E DEFINIÇÕES

Para efeitos deste Regulamento, entende-se por:

- **Dado pessoal**: qualquer informação relativa a uma pessoa singular identificada ou identificável;
- **Tratamento:** qualquer operação realizada sobre dados pessoais, como recolha, registo, conservação, consulta, alteração, divulgação ou eliminação;
- **Responsável pelo tratamento**: o Monte, representado pela sua Administração;
- **Encarregado de Proteção de Dados (EPD):** pessoa designada pelo Monte para monitorizar o cumprimento do RGPD;
- **Titular dos dados**: a pessoa singular a quem os dados dizem respeito.

4. ENTRADA EM VIGOR

O Regulamento Interno de Proteção de Dados Pessoais, entra em vigor a 1 de janeiro de 2026, sendo que as futuras adaptações e melhorias ao mesmo serão previamente discutidas com os trabalhadores e com o EPD, antes de serem incorporadas.

5. ACESSO A DADOS PESSOAIS

Os dados pessoais são propriedade dos respetivos titulares, nomeadamente trabalhadores e restantes pessoas singulares que de uma forma ou outra se relacionam com o **MONTE**, que é a responsável pelo respetivo tratamento.

Por tratamento de dados pessoais deve entender-se a recolha, registo, organização, estruturação, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, comparação ou interconexão, limitação, apagamento ou destruição, pelo que o seu acesso estará limitado apenas aos colaboradores cuja intervenção seja necessária e/ou requerida pelos dirigentes do **MONTE**.

Aos restantes colaboradores é interdito o acesso aos dados pessoais — em papel, em formato digital, vídeo ou qualquer outro disponível — sem autorização dos respetivos dirigentes.

O tratamento de dados pessoais deve respeitar os seguintes princípios:

a) Licitude, lealdade e transparência;

b) Limitação das finalidades;

c) Minimização dos dados;

d) Exatidão e atualização;

e) Limitação da conservação;

f) Integridade e confidencialidade;

g) Responsabilidade (accountability).

O Monte procede ao tratamento de dados pessoais relativos a:

1. **Beneficiários e participantes de projetos:** identificação, contactos, NIF, NISS, dados socioeconómicos, bancários e de empregabilidade;

2. **Formandos e formadores:** identificação, contactos, NIF, NISS, dados bancários, frequência, assiduidade, avaliação e certificação;

3. **Dirigentes e Membros dos Órgãos Sociais, Técnicos, Colaboradores e voluntários**: dados de identificação, contacto, NIF, NISS, dados bancários, remuneração, situação contratual e assiduidade;

4. **Fornecedores e parceiros**: identificação, contactos e dados de faturação.

O tratamento de categorias especiais de dados (ex.: saúde, vulnerabilidade social) só é permitido com consentimento explícito ou com fundamento legal adequado.

6. INFORMAÇÃO E FORMAÇÃO

Todos os colaboradores do **MONTE** têm o direito de estarem informados sobre as medidas de tratamento de dados pessoais realizadas por aquela e os respetivos riscos, bem como das consequências em termos de falhas de segurança.

Todos os colaboradores terão acesso a:

- formação, sensibilizando-os para a importância do cumprimento do presente Regulamento e da Aceder aos dados que lhes digam respeito;
- Solicitar a retificação de dados inexatos;

- Requerer o apagamento dos dados ("direito a ser esquecido");
- Limitar ou opor-se ao tratamento;
- Apresentar reclamação junto da Comissão Nacional de Proteção de Dados (CNPD). Os pedidos devem ser dirigidos ao EPD, através de contacto institucional designado pelo Monte.
- atualizações sobre o sistema de tratamento de dados pessoais;
- receber via correio eletrónico interno, comunicações a alertar para as boas práticas.

Para os trabalhadores com acesso aos dados pessoais existirão sessões periódicas de sensibilização e segurança informáticas, sendo que os seus níveis de proficiência na proteção dos dados pessoais serão revistos anualmente. Caso não sejam satisfatórios, os respetivos níveis de acesso serão revistos ou cancelados, com as respetivas consequências em termos de utilização de equipamentos e acessos a áreas restritas.

7. RESPONSÁVEL PELO TRATAMENTO

O Monte, através da sua Direção, é o responsável pelo tratamento de dados pessoais e garante a adoção de medidas técnicas e organizativas adequadas à sua proteção.

8. ENCARREGADO DE PROTEÇÃO DE DADOS (EDP)

Para executar as tarefas de EPD do MONTE é nomeado o Técnico Superior, Nuno Alexandre Barroso da Costa.

O EPD executa as seguintes funções:

a) Informar e aconselhar a Direção e os colaboradores sobre as suas obrigações legais;

b) Monitorizar o cumprimento do RGPD e do presente Regulamento;

c) Cooperar com a CNPD;

d) Ser ponto de contacto com os titulares dos dados.

O contacto do EPD será divulgado internamente e no website institucional.

9. DEVERES DOS TRABALHADORES, COLBORADORES E VOLUNTÁRIOS

Todos os colaboradores e voluntários devem:

a) Cumprir este Regulamento e as instruções do EPD;

b) Tratar apenas os dados necessários à sua função;

c) Garantir a confidencialidade e segurança das informações;

d) Comunicar de imediato qualquer incidente ou violação de dados.

10. COMUNICAÇÃO COM OS TITULARES DOS DADOS PESSOAIS

Até ao final de 31.12.2025 existirá **uma task force de acompanhamento do processo de implementação do RGPD,** constituída pela Diretora Técnica, Marta Alter, pelos Técnicos Superiores Ana Teresa Silva e Nuno Costa, e pela Técnica Administrativa Rosário Cuba, que terá a seu cargo toda a comunicação com os titulares dos dados pessoais, nomeadamente informando-os sobre:

• A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;

• As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

• As categorias dos dados pessoais em questão.

De igual modo, compete a esta task force gerir todos os pedidos/reclamações/esclarecimentos provenientes dos titulares dos dados pessoais, até à implementação do RGPD que deverá ocorrer a partir de 01.01.2026.

11. UTILIZAÇÃO DE EQUIPAMENTOS

O **MONTE** disponibiliza aos colaboradores equipamentos informáticos de localização fixa, como servidores, desktops e impressoras, e equipamento de utilização móvel como computadores portáteis, tablets, smartphones, pens, discos de memória, etc. Qualquer destes equipamentos que contenham dados pessoais só poderá ser utilizado por colaboradores com nível de acesso aos dados pessoais e para os fins determinados pela Diretora Técnica.

Estes equipamentos, e só estes, terão acesso total à rede wi-fi do **MONTE**. Será alocado, caso a caso, espaço de memória nos equipamentos do **MONTE** para utilização pessoal e confidencial dos colaboradores.

Em áreas restritas, é proibido aos colaboradores trazerem equipamentos Informáticos que não os do **MONTE** sendo expressamente proibida a utilização de dispositivos de armazenamento de dados que não os do **MONTE.**

Os meios informáticos do **MONTE** devem seguir os requisitos técnicos (incluindo as obrigações em relação à capacidade para autenticar e autorizar utilizadores e dispositivos front-end, App, ou camada aplicacional, e base de dados) na arquitetura de segurança das redes e sistemas de informação referenciados pela Resolução do Conselho de Ministros nº 41/2018, publicada em Diário da República, I Série, N.0 62, de 28 de março de 2018.

12. COMUNICAÇÕES DA ENTIDADE

Os equipamentos e software informáticos do **MONTE** não permitirão o acesso a áreas da Internet não essenciais para o trabalho. Assim, passam a estar bloqueados os acessos ao peer-to-peer (ou ponto a ponto), as descargas de programas por utilizadores não autorizados, as redes de wi-fi não pertencentes à empresa, os serviços de correio que não passem pelo servidor (Gmail, outlook, etc.), videojogos, filmes, músicas, redes sociais, etc.

13. PROTEÇÃO DO LOCAL DA DMZ (ZONA DESMILITARIZADA)

Compete ao técnico de informática (a contratar), a gestão da proteção da área que alberga o **MONTE** — servidores, routers, firewalls, sistemas de backup, etc. que poderá passar pela limitação de acesso a pessoas não autorizadas. Qualquer acesso a esta área por pessoa não credenciada — visitantes, inspetores, manutenção, subcontratantes, etc. — deverá ser registado em log próprio. É obrigatória a existência de uma listagem atualizada de quem tem acesso às áreas que contenham dados pessoais.

14. PROTEÇÃO DA REDE INTERNA

A proteção da rede interna onde se localizam os postos de trabalho e eventualmente servidores de aplicações deverá subordinar-se aos requisitos mencionados na Resolução do Conselho de Ministros N.º 41/2018, de 28 de março, no que se refere à autenticação dos utilizadores. Além disto, é interdito aos colaboradores desta área:

- Divulgar a palavra-chave;
- Guardar a palavra-chave em ficheiros abertos ou em papel;
- Registar a palavra-chave nos navegadores;
- Utilizar palavras-chave ligadas aos dados pessoais do utilizador;
- Utilizar a palavra-chave de acesso para outros acessos (redes, outsourcers, ficheiros, etc.);

• Guardar as palavras-chave por defeito (não usar automatismos dos navegadores);

• Enviar as palavras-chave a si mesmo por e-mail;

• Criar ou usar contas partilhadas por vários colaboradores;

• Não apagar as contas de utilizadores que já não estão na empresa;

• Um superior hierárquico esquecer-se de retirar privilégios temporários;

15. PROTEÇÃO DOS DADOS PESSOAIS EM PAPEL

Toda a documentação em papel ou em suportes não informáticos contendo dados pessoais deve estar guardada em gabinete, num armário, inacessível a pessoas não autorizadas e protegida pelos seguintes dispositivos:

• Portas com chave de acesso;

Se alguém tiver acesso temporário a estas áreas de armazenamento, tal deve ficar registado em documento próprio.

16. PROTEÇÃO DE EQUIPAMENTOS MÓVEIS

As regras para a Proteção de Equipamentos Móveis encontram-se descritas no Anexo 2 e fazem parte integrante deste Regulamento.

17. BACKUPS

Todos os dados pessoais sensíveis devem ter um arquivo de backup diário ou semanal (dependendo do volume de tráfego) do tipo incremental. Quanto aos dados pessoais menos sensíveis, os backups deverão ser semanais. (ou quinzenais, dependendo da atividade da Entidade)

Os backups digitais deverão ser guardados em armários fechados e de acesso restrito.

Quanto aos dados pessoais em papel e que não possam ou não devam ser digitalizados, os mesmos devem ser guardados em armários fechados e de acesso restrito.

O responsável pela realização dos backups deve ter atenção ao prazo de validade dos respetivos dispositivos.

18. RASTREAMENTO DE ACESSOS E GESTÃO DE INCIDENTES

Os servidores do **MONTE** possuem dispositivos gestores de rastreio e de memória confidencial de e-mails, por forma a produzirem o seguinte tipo de informação:

• Um jornal de logs (conservado por um período máximo de seis meses);

• Quem utilizou (login), com data e hora, detalhando-se também o logout ou saída do sistema;

• Os e-mails enviados pelos colaboradores (no exercício das suas funções) geram uma cópia automática (será arquivada em servidor próprio), só podendo ser acedidos em caso de incidente ou para inspeção pela Comissão Nacional de Proteção de Dados, e serão destruídos, um ano após o trabalhador ter cessado as suas funções na Entidade;

Em caso de incidente (roubo, perda de DR, vírus informático, etc.), é obrigatório por parte de qualquer trabalhador do **MONTE** comunicar, de imediato ao seu superior hierárquico, detalhando que tipo de ficheiro ou dado pessoal foi afetado. Para tal, os utilizadores devem possuir listas de nomes a contactar. Por sua vez, o responsável deverá respeitar os procedimentos requeridos pelo RGPD.

19. SUBCONTRATAÇÃO

O **MONTE** só subcontratará tratamento de dados pessoais com entidades credíveis, responsáveis e que respeitem integralmente o RGPD, mediante a assinatura de contratos de subcontratação que obedeçam aos modelos existentes na Entidade. Assim, o Conselho de Administração exige que, antes da celebração de tais contratos, lhe seja apresentado um relatório escrito que garanta que o subcontratante apresenta garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma que o tratamento satisfaça os requisitos do RGPD.

20. RELAÇÕES LABORAIS

O RGPD em nada altera as relações laborais existentes no **MONTE** apenas coloca os trabalhadores no mesmo plano de privacidade que qualquer outro titular de dados.

Neste sentido, o **MONTE** colocará em prática, e em todas as ocasiões em que tal se revele necessário, as devidas restrições com relação à videovigilância, aos chamados dados sensíveis, à utilização de equipamentos de rastreio via Internet das Coisas (IOT) ou a quaisquer novas tecnologias que possam ser intrusivas da privacidade dos nossos trabalhadores.

Arraiolos, 27 de novembro de 2025