ÍNDICE

I. BREVE ENQUADRAMENTO 9
Da Diretiva 95/46/CE ao Regulamento (UE) 2016/679: os principais pontos de contacto e as principais novidades 9

II. CARACTERIZAÇÃO DA ENTIDADE E ORÇAMENTAÇÃO DOS TRABALHOS 15
1. Contacto com a entidade 15
2. Identificação dos sistemas implementados 16
3. Identificação preliminar das necessidades 16

III. PROCESSO DE ADEQUAÇÃO AO RGPD EM TRÊS FASES 19
A. Fase 1: Auditoria inicial: diagnóstico e mapeamento dos dados 19
1. Identificação das operações com dados pessoais 19
2. Inventariação dos dados pessoais 23
3. Inventariação dos intervenientes que processam dados pessoais 26
4. Inventariação dos fluxos de dados 28
5. Identificação das medidas de segurança existentes 28
6. Identificação dos riscos de privacidade 29
7. Avaliação do mérito das operações realizadas 30
8. Avaliação da forma das operações realizadas 32
9. Verificação dos requisitos de licitude do tratamento 33
10. Identificação das áreas e dimensões necessárias de atuação 34

B. Fase 2: Descrição das medidas a tomar para a adequação 35
1. Desenvolvimento de um cronograma de atuação e de investimento 35

2. Medidas para assegurar os direitos dos titulares dos dados 36
3. Adequação das operações com dados face às finalidades do tratamento 40
4. Adequação das operações sob o princípio da privacidade desde a conceção 41
5. Identificação das opções existentes de sistemas e serviços 43
6. Análise dos sítios, plataformas, sistemas e similares detidos e/ou utilizados pela entidade 45
7. Análise dos contratos existentes 49
8. Levantamento de informações junto dos prestadores de serviços da entidade 51
9. Desenvolvimento dos suportes de recolha de dados 53
10. Desenvolvimento dos suportes de registo das atividades de tratamento 53
11. Desenvolvimento de guia de procedimentos internos 54
12. Desenvolvimento da política de tratamento de dados pessoais da entidade 55

C. Fase 3: Implementação das medidas necessárias para cumprimento 56
1. Aplicação das recomendações resultantes do relatório da fase 2 56
2. Utilização dos documentos produzidos no âmbito da fase 2 56
3. Acordos sobre responsabilidades no tratamento de dados com os subcontratantes e outros 57
4. Aditamentos aos contratos existentes e celebração de novos contratos (escritos) 62
5. Adequação dos sítios e/ou aplicações em linha 64
6. Divulgação e aplicação das políticas desenvolvidas e procedimentos recomendados 65
7. Cumprimento do dever de informação aos titulares dos dados 66
8. Cumprimento do dever de informação a todas as entidades 68
9. Implementação de mecanismos de licitude do tratamento válidos 69
10. Implementação de monitorização e controlos adequados 73
11. Nomeação de um responsável pela proteção de dados ou de um encarregado da proteção de dados 74
12. Implementação de sistemas de gestão de segurança da informação 74

13. Registo dos procedimentos e medidas promovidas para demonstração da adequação 78
14. Relatório final 78

IV. PÓS-ADEQUAÇÃO AO RGPD: O PAPEL DO ENCARREGADO DA PROTEÇÃO DE DADOS 81
1. A importância da existência de um responsável da proteção de dados 88
2. A obrigatoriedade de nomeação de encarregado da proteção de dados 91
3. Outros casos de nomeação de encarregado da proteção de dados 94
4. Nomeação de encarregado da proteção de dados interno ou externo à entidade 95
5. A nomeação junto da Autoridade de Controlo 98
6. A importância da formação interna e da sensibilização para as questões da privacidade e segurança 100
7. O registo das atividades de tratamento de dados 102
8. A fiscalização sucessiva 103
9. A(s) auditoria(s) de conformidade 104
10. A promoção de testes regulares de vulnerabilidades e a violação da privacidade 107
11. O parecer nas avaliações de impacto da proteção de dados 108
12. A comunicação de violações da privacidade 114
    A) À Autoridade de Controlo (CNPD) 114
    B) Aos titulares dos dados pessoais 116

V. ANEXOS 121
Anexo I Caraterização da entidade a auditar 123
Anexo II Guia da auditoria inicial em proteção de dados 125
Anexo III Índice da política de privacidade e tratamento de dados pessoais 133
Anexo IV Acordo de regulação de responsabilidades em termos de tratamento de dados pessoais – subcontratantes 137
Anexo V Acordo de regulação de responsabilidades em termos de tratamento de dados pessoais – responsáveis conjuntos 143
Anexo VI Aditamento a contrato de trabalho 147

Anexo VII Aditamento a contrato de prestação de serviços – pessoa singular 151
Anexo VIII Aditamento a contrato de prestação de serviços – empresa 155
Anexo IX Exemplo de texto informativo aos parceiros negociais ou prestadores de serviços 157
Anexo X Declaração de consentimento para tratamento de dados pessoais (recrutamento) 159
Anexo XI *Email* tipo para consentimento no tratamento das candidaturas espontâneas 161
Anexo XII Procedimento de envio de *newsletters* ou outras subscrições 163
Anexo XIII *Email* tipo para envio de *newsletters* ou outras subscrições 165
Anexo XIV Índice do relatório final de adequação ao regulamento geral sobre a proteção de dados 167
Anexo XV Avaliação de impacto sobre a proteção de dados – *check list* 169
Anexo XVI Modelo complementar à *check list* da avaliação de impacto sobre a proteção de dados 173