ÍNDICE

Prefácio 17

Nota introdutória 21

Símbolos usados 25

Glossário 27

Siglas e acrónimos 33

PARTE I O PAPEL DO DEPARTAMENTO DE RECURSOS HUMANOS NA CONFORMIDADE COM O RGPD 35

PARTE II COMO ESTÁ ORGANIZADO O GUIA PRÁTICO? 43

PARTE III GUIA PRÁTICO PARA A CONFORMIDADE COM O RGPD 63

III.AT. Aspetos transversais da conformidade com o RGPD 63

III.AT.1. Exercício de direitos por parte dos titulares de dados pessoais 63

III.AT.1.1. Enquadramento jurídico 64

Que direitos de proteção de dados pessoais podem ser exercidos por um trabalhador junto do seu empregador? 64

Direito à informação: prestação de informação aos titulares dos dados (trabalhadores) 65

Qual o dever do empregador, enquanto responsável pelo tratamento, face a um pedido de exercício de direitos? 66

III.AT.1.2. Auditoria e recomendações para a conformidade – RGPD 67

Requisitos ISO 27001 e RGPD 67

Objetivos de controlo 68

Avaliação de riscos 69
Sugestão de medidas de controlo a implementar 70
III.AT.2. Incidentes de segurança da informação e de proteção de dados pessoais, e regime sancionatório 73
III.AT.2.1. Enquadramento jurídico 73
Regime contraordenacional previsto na Lei de Execução 76
III.AT.2.2. Auditoria e recomendações para a conformidade – RGPD 78
Requisitos ISO 27001 e RGPD 78
Objetivos de controlo 78
Avaliação de riscos 79
Sugestão de medidas de controlo a implementar 80
III.AT.3. Nomeação e funções do encarregado da proteção de dados 83
III.AT.3.1. Enquadramento jurídico 83
Designação do EPD 83
Competências e conhecimentos especializados do EPD 85
Modelo de comunicação com o EPD 87
Funções do EPD 88
Responsabilidade civil profissional do EPD 90
III.AT.3.2. Auditoria e recomendações para a conformidade – RGPD 91
Requisitos ISO 27001 e RGPD 91
Objetivos de controlo 91
Avaliação de riscos 92
Sugestão de medidas de controlo a implementar 93
III.AT.4. Avaliação de impacto para a proteção de dados pessoais (AIPD) 95
III.AT.4.1. Enquadramento jurídico 95
Realização de uma AIPD 96
Realização de uma consulta prévia à autoridade de controlo 96
III.AT.4.2. Auditoria e recomendações para a conformidade – RGPD 98
Requisitos ISO 27001 e RGPD 98
Objetivos de controlo 99
Avaliação de Riscos 99
Sugestão de medidas de controlo a implementar 100
III.AT.5. Subcontratação e responsabilidades – RGPD 101
III.AT.5.1. Enquadramento jurídico 102
A figura do subcontratante para o RGPD 102
Acordos de subcontratação no âmbito da relação laboral 103
Dever de informar os trabalhadores dos subcontratantes utilizados no âmbito da relação laboral 105

Direito de indemnização e responsabilidade civil do responsável pelo tratamento e do subcontratante 105
III.AT.5.2. Auditoria e recomendações para a conformidade – RGPD 106
Requisitos ISO 27001 e RGPD 106
Objetivos de controlo 106
Avaliação de riscos 107
Sugestão de medidas de controlo a implementar 108

III.RH. Conformidade com o RGPD nos tratamentos de dados dos RH

... até à formalização do contrato (diligências pré-contratuais) 110
III.RH.1. Seleção e recrutamento/receção e tratamento de *curricula vitae* 110
III.RH.1.1. Enquadramento jurídico 110
O que podemos perguntar a um candidato a emprego? Que documentos/certificados podemos pedir? Podemos armazenar esses dados? Até quando? 110
Que interesses poderão então justificar a compressão do direito à privacidade dos candidatos a emprego? 111
Background checks 112
Recrutamento *online* 113
Recrutamento eletrónico/Definição de perfis 114
Serviços de apoio à distância e *call centres* 115
Podemos armazenar os dados referentes a um processo de recrutamento? Até quando? 115
Elementos a fazer constar de um modelo de declaração informativa relativa à recolha e tratamento de dados pessoais no âmbito de um processo de seleção e recrutamento 118
Finalidades do tratamento de dados pessoais no âmbito de um processo de seleção e recrutamento 118
Fundamentos para o tratamento de dados pessoais no âmbito de um processo de seleção e recrutamento 118
Categorias de dados pessoais do trabalhador a tratar 119
Transferências de dados para terceiros 119
Os direitos do candidato a emprego 121
Período de retenção 121
Medidas de Segurança 121
Contactos 121
Direito a apresentar queixa perante a autoridade de controlo 121

III.RH.1.2. Auditoria e recomendações para a conformidade – RGPD 122
Receção e tratamento de *curricula vitae* 122
Requisitos ISO 27001 e RGPD 122
Objetivos de controlo 122
Avaliação de riscos 123
Sugestão de medidas de controlo a implementar 123
Processo de seleção e recrutamento 125
Requisitos ISO 27001 e RGPD 125
Objetivos de controlo 125
Avaliação de riscos 126
Sugestão de medidas de controlo a implementar 126
III.RH.2. Recolha e tratamento de dados pessoais com vista à contratação laboral 127
III.RH.2.1. Enquadramento jurídico 127
Das finalidades para o tratamento de dados pessoais dos trabalhadores 127
Fundamentos para o tratamento de dados pessoais no âmbito da relação laboral 129
O consentimento dos trabalhadores 130
III.RH.2.2. Auditoria e recomendações para a conformidade – RGPD 132
Requisitos ISO 27001 e RGPD 132
Objetivos de controlo 133
Avaliação de riscos 133
Sugestão de medidas de controlo a implementar 134
III.RH.3. Contratação (diligências para) 134
III.RH.3.1. Enquadramento jurídico 134
Finalidade do tratamento e fundamento jurídico específico 135
Categorias de dados a tratar no âmbito da relação de trabalho 136
Dados pessoais de terceiros 138
Utilização de subcontratantes / Dever de informação a prestar aos trabalhadores 139
III.RH.3.2. Auditoria e recomendações para a conformidade – RGPD 139
Requisitos ISO 27001 e RGPD 139
Objetivos de controlo 140
Avaliação de riscos 140
Sugestão de medidas de controlo a implementar 141

... durante a relação laboral 143
III.RH.4. Sensibilização e compromisso com regulamentos e regras de conduta 143
III.RH.4.1. Enquadramento jurídico 143
Normas internas: regulamentos e regras de conduta 143

III.RH.4.2. Auditoria e recomendações para a conformidade – RGPD 144
Requisitos ISO 27001 e RGPD 144
Objetivos de controlo 145
Avaliação de riscos 145
Sugestão de medidas de controlo a implementar 146
III.RH.5. Atribuição de acessos físicos e acessos aos sistemas informáticos 148
III.RH.5.1. Enquadramento jurídico 148
Fundamento 148
Enquadramento legal 149
Controlo do *email* dos trabalhadores 149
Monitorização do uso da internet 150
Acesso remoto ao computador do trabalhador 150
Controlo de dados de comunicações telefónicas e de tráfego 151
III.RH.5.2. Auditoria e recomendações para a conformidade – RGPD 151
Requisitos ISO 27001 e RGPD 151
Objetivos de controlo 152
Avaliação de riscos 152
Sugestão de medidas de controlo a implementar 153
III.RH.6. Atribuição de equipamentos informáticos e dispositivos eletrónicos 155
III.RH.6.1. Enquadramento jurídico 155
III.RH.6.2. Auditoria e recomendações para a conformidade – RGPD 156
Requisitos ISO 27001 e RGPD 156
Objetivos de controlo 156
Avaliação de riscos 157
Sugestão de medidas de controlo a implementar 157
III.RH.7. Gestão de horários, turnos e escalas 158
III.RH.7.1. Enquadramento jurídico 158
III.RH.7.2. Auditoria e recomendações para a conformidade – RGPD 160
Requisitos ISO 27001 e RGPD 160
Objetivos de controlo 160
Avaliação de riscos 161
Sugestão de medidas de controlo a implementar 161
III.RH.8. Gestão de férias, ausências e justificação 162
III.RH.8.1. Enquadramento jurídico 162
Fundamento de licitude 162
Faltas e sua justificação 163
III.RH.8.2. Auditoria e recomendações para a conformidade – RGPD 165
Requisitos ISO 27001 e RGPD 165

Objetivos de controlo 165
Avaliação de riscos 165
Sugestão de medidas de controlo a implementar 166
III.RH.9. Segurança, higiene e saúde no trabalho 167
III.RH.9.1. Enquadramento jurídico 167
Tratamento de dados pessoais para efeitos de segurança e saúde no trabalho 167
Controlo de alcoolemia e de consumo de estupefacientes 168
Ação dos responsáveis pela segurança, higiene e saúde no trabalho 170
III.RH.9.2. Auditoria e recomendações para a conformidade – RGPD 170
Requisitos ISO 27001 e RGPD 170
Objetivos de controlo 171
Avaliação de riscos 171
Sugestão de medidas de controlo a implementar 172
III.RH.10. Publicações de reporte obrigatório 173
III.RH.10.1. Enquadramento jurídico 173
III.RH.10.2. Auditoria e recomendações para a conformidade – RGPD 174
Requisitos ISO 27001 e RGPD 174
Objetivos de controlo 174
Avaliação de riscos 175
Sugestão de medidas de controlo a implementar 175
III.RH.11. Processamento salarial 177
III.RH.11.1. Enquadramento jurídico – Código do Trabalho 177
Fundamento de licitude 177
Utilização de um subcontratante para o processamento salarial 177
III.RH.11.2. Auditoria e recomendações para a conformidade – RGPD/ Código do Trabalho 179
Requisitos ISO 27001 e RGPD 179
Objetivos de controlo 179
Avaliação de riscos 180
Sugestão de medidas de controlo a implementar 181
III.RH.12. Seguros para trabalhadores 183
III.RH.12.1. Enquadramento jurídico 183
III.RH.12.2. Auditoria e recomendações para a conformidade – RGPD 183
Requisitos ISO 27001 e RGPD 184
Objetivos de controlo 184
Avaliação de riscos 184
Sugestão de medidas de controlo a implementar 185
III.RH.13. Divulgação dos contactos de trabalhadores a terceiros 186
Qual a legitimidade do empregador, e dos seus trabalhadores, para divulgar contactos, pessoais e profissionais, dos trabalhadores junto de terceiros? 186

III.RH.13.1. Enquadramento jurídico 187
III.RH.13.2. Auditoria e recomendações para a conformidade – RGPD 187
Requisitos ISO 27001 e RGPD 188
Objetivos de controlo 188
Avaliação de riscos 188
Sugestão de medidas de controlo a implementar 189
III.RH.14. Atribuição de veículo automóvel, equipamentos de identificação e georreferenciação 190
III.RH.14.1. Enquadramento jurídico 192
Necessidade de realizar uma avaliação de impacto sobre a proteção de dados pessoais (AIPD) 193
Pedido de parecer à comissão de trabalhadores 194
Celebração de acordo de subcontratação do tratamento de dados pessoais 194
Prestação de informação aos titulares dos dados (trabalhadores) 194
Atualização do registo das atividades de tratamento 195
III.RH.14.2. Auditoria e recomendações para a conformidade – RGPD 196
Requisitos ISO 27001 e RGPD 196
Objetivos de controlo 196
Avaliação de riscos 197
Sugestão de medidas de controlo a implementar 197
III.RH.15. Arquivo da ficha individual do trabalhador 198
III.RH.15.1. Enquadramento jurídico 199
III.RH.15.2. Auditoria e recomendações para a conformidade – RGPD 200
Requisitos ISO 27001 e RGPD 200
Objetivos de controlo 201
Avaliação de riscos 202
Sugestão de medidas de controlo a implementar 202
III.RH.16. Recolha, tratamento e divulgação da imagem de trabalhadores 204
III.RH.16.1. Enquadramento jurídico 205
Minuta de declaração/Pedido de consentimento 205
III.RH.16.2. Auditoria e recomendações para a conformidade – RGPD 206
Requisitos ISO 27001 e RGPD 206
Objetivos de controlo 206
Avaliação de riscos 207
Sugestão de medidas de controlo a implementar 207
III.RH.17. Videovigilância (CCTV) 208
III.RH.17.1. Enquadramento jurídico e Código do Trabalho 209
Finalidades legalmente admissíveis 210

Dever de informação aos trabalhadores (e a outros titulares de dados) 211
Obrigações a cumprir aquando da instalação de um sistema de videovigilância 212
Locais objeto de videovigilância 212
Processo de instalação de dispositivo de videovigilância 213
Pedido de autorização à CNPD? 214
Pedido de parecer à comissão de trabalhadores 214
A utilização das imagens recolhidas: usos permitidos 215
Utilização de imagens de videovigilância para fins disciplinares 215
III.RH.17.2. Auditoria e recomendações para a conformidade – RGPD 217
Requisitos ISO 27001 e RGPD 217
Objetivos de controlo 217
Avaliação de riscos 218
Sugestão de medidas de controlo a implementar 219
III.RH.18. Utilização de dados biométricos de trabalhadores no âmbito da relação laboral 221
III.RH.18.1. Enquadramento jurídico 221
Processo de instalação/utilização de dispositivos de biometria 223
Abolição do pedido de notificação à CNPD 223
Dever de informação em matéria de dados biométricos 224
Pedido de parecer à comissão de trabalhadores 225
III.RH.18.2. Auditoria e recomendações para a conformidade – RGPD 226
Requisitos ISO 27001 e RGPD 226
Objetivos de controlo 226
Avaliação de riscos 227
Sugestão de medidas de controlo a implementar 228
III.RH.19. A gravação de chamadas telefónicas e o seu impacto nas relações laborais 229
III.RH.19.1. Enquadramento jurídico 229
As chamadas telefónicas que realizamos no local de trabalho podem ser gravadas? 229
Chamadas pessoais *versus* chamadas profissionais 230
Qual o enquadramento legal aplicável? 230
A validade da Deliberação n.º 629/2010 da Comissão Nacional de Proteção de Dados 231
Tratamento de dados pessoais decorrentes da gravação de chamadas, efetuada no âmbito da monitorização da qualidade do atendimento 231
Fundamentos para a recolha de dados dos trabalhadores para efeitos de gravação de chamadas 233
Tratamento de dados pessoais decorrente da gravação de chamadas efetuada no âmbito de uma relação contratual 235

Tratamento de dados pessoais decorrentes da gravação de chamadas efetuada no âmbito de uma situação de emergência 236
Prazo de conservação das gravações 237
Subcontratante 237
III.RH.19.2. Auditoria e recomendações para a conformidade – RGPD 238
Requisitos ISO 27001 e RGPD 238
Objetivos de controlo 238
Avaliação de riscos 239
Sugestão de medidas de controlo a implementar 240
III.RH.20. Teletrabalho 240
III.RH.20.1. Enquadramento jurídico 241
Conceito 241
Nem todo o teletrabalho é igual 242
Instrumentos de trabalho 242
Controlo de assiduidade e da pontualidade 243
Outros controlos à distância 243
III.RH.20.2. Auditoria e recomendações para a conformidade – RGPD 244
Requisitos ISO 27001 e RGPD 244
Objetivos de controlo 244
Avaliação de riscos 245
Sugestão de medidas de controlo a implementar 248
III.RH.21. Monitorização da temperatura corporal dos trabalhadores 251
III.RH.21.1. Enquadramento jurídico 252
Posição da CNPD 252
Opção legislativa 252
Temperatura normal? 253
Dever de informação aos trabalhadores 254
Legitimidade para proceder à monitorização da temperatura dos trabalhadores 254
III.RH.21.2. Auditoria e recomendações para a conformidade – RGPD 255
Requisitos ISO 27001 e RGPD 255
Objetivos de controlo 255
Avaliação de riscos 256
Sugestão de medidas de controlo a implementar 257
III.RH.22. Sanções disciplinares 258
III.RH.22.1. Enquadramento jurídico 259
III.RH.22.2. Auditoria e recomendações para a conformidade – RGPD 260
Requisitos ISO 27001 e RGPD 260
Objetivos de controlo 260

Avaliação de riscos 261
Sugestão de medidas de controlo a implementar 261
III.RH.23. Tratamento de dados de condenações penais e de diversas infrações 263
III.RH.23.1. Enquadramento jurídico 264
III.RH.23.2. Auditoria e recomendações para a conformidade – RGPD 266
Requisitos ISO 27001 e RGPD 266
Objetivos de controlo 267
Avaliação de riscos 267
Sugestão de medidas de controlo a implementar 268
III.RH.24. Tratamento de dados de menores 269
III.RH.24.1. Enquadramento jurídico 269
Tratamento de dados de terceiros – descendentes dos trabalhadores 270
Contactos de terceiros para situações de emergência 271
III.RH.24.2. Auditoria e recomendações para a conformidade – RGPD 272
Requisitos ISO 27001 e RGPD 272
Objetivos de controlo 272
Avaliação de riscos 273
Sugestão de medidas de controlo a implementar 273
III.RH.25. Linhas de ética e prevenção/combate ao assédio no local de trabalho 275
III.RH.25.1. Enquadramento jurídico 275
Fundamentos jurídicos aplicáveis 277
Pedido de parecer à comissão de trabalhadores 277
Realização de uma avaliação de impacto sobre a proteção de dados (AIPD) 277
Prazos de conservação 278
III.RH.25.2. Auditoria e recomendações para a conformidade – RGPD 278
Requisitos ISO 27001 e RGPD 278
Objetivos de controlo 279
Avaliação de riscos 280
Sugestão de medidas de controlo a implementar 281
III.RH.26. Alteração de funções e de responsabilidades 283
III.RH.26.1. Enquadramento jurídico 283
III.RH.26.2. Auditoria e recomendações para a conformidade – RGPD 284
Requisitos ISO 27001 e RGPD 284
Objetivos de controlo 285
Avaliação de riscos 285
Sugestão de medidas de controlo a implementar 286

Diligências com vista à cessação contratual 288
III.RH.27. Cessação do contrato de trabalho 288
III.RH.27.1. Enquadramento jurídico 288
III.RH.27.2. Auditoria e recomendações para a conformidade – RGPD 289
Requisitos ISO 27001 e RGPD 289
Objetivos de controlo 290
Avaliação de riscos 290
Sugestão de medidas de controlo a implementar 291
III.RH.28. Entrega de bens e cessação de acessos físicos e lógicos 292
III.RH.28.1. Enquadramento jurídico 292
Entrega das ferramentas de trabalho 292
Conteúdo da caixa de correio eletrónico (*email*) 292
III.RH.28.2. Auditoria e recomendações para a conformidade – RGPD 292
Requisitos ISO 27001 e RGPD 293
Objetivos de controlo 294
Avaliação de riscos 294
Sugestão de medidas de controlo a implementar 295
III.RH.29. Retenção e destruição dos dados 296
III.RH.29.1. Enquadramento jurídico 296
Princípios a ter conta no tocante à conservação dos dados 298
Direito ao apagamento – direito diferido no tempo 300
Alternativas ao apagamento dos dados 301
Prazos de conservação 301
III.RH.29.2. Auditoria e recomendações para a conformidade – RGPD 302
Requisitos ISO 27001 e RGPD 302
Objetivos de controlo 302
Avaliação de riscos 303
Sugestão de medidas de controlo a implementar 304

BIBLIOGRAFIA 307