Proteção e Tratamento de Dados Pessoais na Hotelaria

Pedro Baptista
2018

Proteção e Tratamento de Dados Pessoais na Hotelaria

Pedro Baptista

Relatório de Estágio para obtenção do Grau de Mestre em Gestão e Direção Hoteleira

Relatório de estágio realizado sob a orientação do Professor Doutor Paulo Jorge Almeida, Professor da Escola Superior de Turismo e Tecnologia do Mar do Instituto Politécnico de Leiria

2018

Agradecimentos

Um agradecimento especial ao Professor Doutor Paulo Jorge Almeida, Professor da Escola Superior de Turismo e do Mar de Peniche e ao Doutor Gonçalo Rebelo de Almeida, administrador do grupo Vila Galé, pela orientação e acompanhamento deste estágio.

Uma saudação a todos os professores e alunos do Mestrado de Direção e Gestão Hoteleira da Escola Superior de Turismo e do Mar de Peniche e a todos os colaboradores do Grupo Vila Galé pela cordialidade e simpatia.

Um beijo à Ana e aos meus pais.

Resumo

Este trabalho é o resultado de um estágio curricular realizado no Grupo Vila Galé, no âmbito do Mestrado em Gestão e Direção Hoteleira da Escola Superior de Turismo e Tecnologia do Mar do Instituto Politécnico de Leiria.

Este estágio decorreu na Sede do Grupo Vila Galé em Entrecampos, Lisboa, e no Departamento de Direção do Hotel Vila Galé Ópera entre setembro de 2017 e julho de 2018.

A Vila Galé é um grupo hoteleiro que opera de acordo com os princípios e padrões de serviço mais elevados. Um desses princípios é a proteção da privacidade dos seus clientes, colaboradores e fornecedores. Neste relatório é apresentada uma análise ao tema da Proteção e Tratamento Dados Pessoais na hotelaria, são descritas as medidas propostas com vista à conformidade com o Regulamento Geral de Proteção de Dados e analisados os seus efeitos na operação hoteleira.

O relatório inicia-se com a apresentação do tema e com a caracterização do Grupo Vila Galé. Segue-se a descrição das atividades realizadas no âmbito do estágio e do projeto desenvolvido, a conclusão e a análise crítica.

Palavras-Chave: Estágio, Gestão Hoteleira, RGPD, Proteção de Dados

Abstract

This article reports an internship at the Vila Galé Group, within a Masters in Hospitality Management of the Escola Superior de Turismo e Tecnologia do Mar, Instituto Politécnico de Leiria.

This internship took place at the headquarters of the Vila Galé Group, in Entrecampos, Lisbon, and at the Management Department of the Hotel Vila Galé Ópera between September 2017 and July 2018.

Vila Galé operates according to the highest standards of service. One of which is protecting the privacy of its customers, employees and suppliers. This report analyses the processing and protection of personal data in the hotel industry, depicts a set of measures proposed to comply with the General Data Protection Regulation and analyses its effects on the hotel operation.

The report begins with the presentation of the theme and the characterization of Vila Galé Group. Afterword's it describes the activities and the developed project, end notes and critical analysis.

Keywords: Internship; Hospitality Management; GDPR; Data Protection

Índice de Conteúdos

Índice de Figuras

Índice de Tabelas

Lista de Siglas

CNPD - Comissão Nacional de Proteção de Dados

DPO – Data *Protection Officer* (Encarregado de Proteção dos Dados)

DPIA - *Data Protection Impact Assessment (*Avaliação de Impacto da Privacidade de Dados)

ERP – *Enterprise Resource Planning*

ESTM – Escola Superior de Turismo e Tecnologia do Mar

GDH – Gestão e Direção Hoteleira

GDPD – *General Data Protection Regulation* (ou Regulamento Geral de Proteção de Dados)

IPL – Instituto Politécnico de Leiria

OTA – *Online Travel Agency*

RGPD – Regulamento Geral de Proteção de Dados

1. Introdução

Este estágio curricular foi inserido no âmbito no segundo ano do Mestrado em Gestão e Direção Hoteleira da Escola Superior de Turismo e Tecnologia do Mar do Instituto Politécnico de Leiria e permitiu consolidar os conhecimentos adquiridos no primeiro ano do Mestrado.

O serviço de hospedagem consiste no alojamento com ou sem refeição em que o valor da prestação reside na natureza da performance do hoteleiro e do envolvimento do consumidor com o processo, com os outros clientes e com as estruturas físicas nas quais o serviço é prestado.

No caso das pequenas e médias empresas hoteleiras o gestor tem um papel funcional mais concentrado. As suas funções de direção, coordenação e controlo tendem a fundir-se, sendo a tomada de decisão tendencialmente mais informal e imediata. No caso das grandes empresas, compostas por várias unidades de negócio, e muitas vezes com localizações dispersas, o gestor tende a focar-se na gestão de processos internos e em relações públicas formulando e implementando objetivos estratégicos, num processo de elaboração no qual se define a relação entre a organização, e o ambiente interno e externo[1].

Nos últimos anos tem-se assistido a um crescimento global do sector dos serviços. A hotelaria e o turismo são um dos principais fatores que contribuem para este facto. Em Portugal, segundo dados do Instituto Nacional de Estatística de fevereiro de 2018, a hotelaria registou em 2017, mais de vinte milhões de hóspedes e 57 milhões de dormidas, o que corresponde a um aumento anual de 8,9% e de 7,4%, respetivamente, em 2017, e de 9,2% e 9,6% em 2016, com os proveitos totais a aumentarem em 16,6% em 2017 e 17,3% em 2016 [2].

Estes resultados são acompanhados do proliferar de novos serviços de mediação como as agências de viagem *online* ou o *Airbnb,* e de mudanças nos modelos de distribuição, de gestão da comunicação e dos canais de vendas aos quais a livre circulação de informação comercial e de Dados Pessoais são condição essencial.

---

[1] Batenman, Snell (1998). Administração: Construindo Vantagem Competitiva. São Paulo: Atlas

[2] Instituto Nacional de Estatística (2017). "Resultados preliminares de 2017: crescimentos de 8,9% nos hóspedes e 7,4% nas dormidas". Disponível em https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=DESTAQUE

De forma a poder oferecer um entendimento combinado de todas estas realidades, este estágio envolveu um *cross training* nos Departamentos Jurídico, Marketing, Reservas, *Revenue*, Vendas Comerciais, Compras e de Administração do Grupo Vila Galé e nos Departamentos de Direção do Hotel Vila Galé Ópera o que permitiu um contacto com uma multiplicidade de dimensões e de tarefas.

1.1. Objetivos

O estágio curricular contribui para a aquisição e desenvolvimento de conhecimentos e competências profissionais necessárias ao desempenho de uma atividade profissional. O estágio curricular permite, por um lado, um contacto direto com os postos de trabalho, as funções, e as rotinas inerentes à direção hoteleira, e por outro lado, permite uma aculturação ao esquema empresarial e social da organização.

Este estágio teve como objetivo geral colaborar na implementação do novo Regulamento Geral de Proteção de Dados que a partir de maio de 2018 veio regular os processos de tratamento de Dados Pessoais realizado por empresas e entidades públicas.

De forma a avaliar se o objetivo geral foi alcançado foram definidos três objetivos específicos:

- O primeiro objetivo específico foi interpretar o novo Regulamento Geral de Proteção de Dados Pessoais, enumerar os requisitos legais (substanciais e formais) impostos às empresas em geral, e aos hotéis em particular, e desenhar um conjunto de medidas e boas práticas para os satisfazer;

- O segundo objetivo foi caracterizar a estrutura, as funções e a natureza dos fluxos da informação dentro das empresas hoteleiras, e as relações entre os diversos departamentos centrais e os hotéis;

- O terceiro objetivo foi desenvolver e propor a implementação de um conjunto de medidas que garantissem a conformidade das operações de tratamento de Dados Pessoais com os requisitos impostos pelo Regulamento.

1.2. Estrutura do Relatório

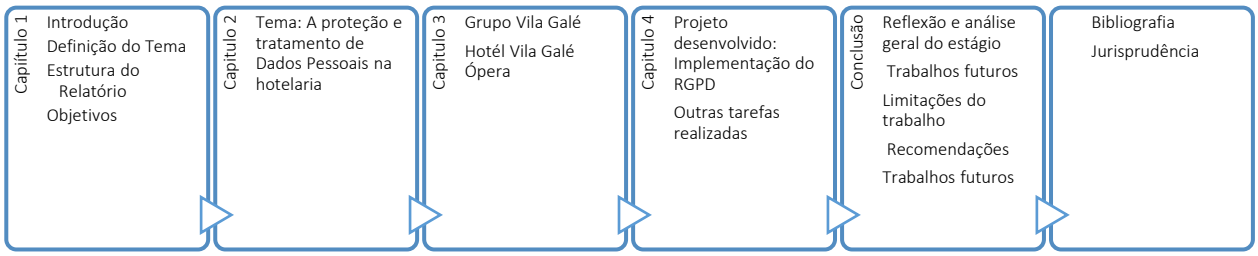

Tabela 1 "Estrutura do Relatório" (Fonte Própria, 2018)

No Capítulo 1 é introduzido o tema, a estrutura do relatório, o objetivo geral e os objetivos específicos do estágio.

No Capítulo 2 é desenvolvido o tema do projeto em conjunto com as referências bibliográficas.

No Capítulo 3 é caracterizada a cadeia hoteleira e os hotéis onde foi realizado o estágio.

No Capítulo 4 são descritas as tarefas e o projeto realizado durante o estágio.

Na Conclusão são analisadas as limitações levantadas durante a implementação do RGPD e são sugeridas medidas futuras e propostas de investigação acerca do tema.

2. Tema: A proteção e tratamento de Dados Pessoais na hotelaria

2.1. Proteção de Dados Pessoais

A circulação de Dados Pessoais é essencial à prossecução da generalidade das atividades económicas e das liberdades comunitárias - livre circulação de bens, livre circulação de serviços e livre circulação de capitais – e dos pilares do mercado económico comum europeu. Independentemente da possibilidade da sua monetarização - como qualquer outro bem – a circulação de Dados Pessoais é essencial às atividades económicas e promove um conjunto alargado de benefícios públicos.

Por um lado, os Dados Pessoais permitem identificar os intervenientes comerciais, preparar diligências pré-contratuais e executar os contratos nos quais os titulares dos dados são parte. Sem a recolha e a partilha de Dados Pessoais, não é possível, por exemplo, celebrar um número significativo de contratos de compra e venda, prestações

de serviços ou contratos de trabalho. No caso da indústria hoteleira, os Dados Pessoais são condição essencial para celebrar os contratos de hospedagem assim com outros serviços conexos (serviços e tratamentos de saúde e bem-estar, serviços de *rent-a-car*, programas de fidelização, etc.).

Para além disso, a recolha de Dados Pessoais pode ser necessária para o cumprimento de obrigações jurídicas a que o hoteleiro está sujeito por lei. No caso português, por exemplo, a recolha de Dados Pessoais é obrigatória para efeitos de faturação nos termos do Decreto-Lei n.º 197/2012 de 24 de agosto, assim como, para o preenchimento dos boletins de alojamento, que se destinam a permitir o controlo dos cidadãos estrangeiros e posterior comunicação ao Serviços de Estrangeiros e Fronteiras nos termos do artigo 15.º da Lei n.º 23/2007, de 4 de julho.

Por outro lado, os Dados Pessoais são um ativo que permite às empresas desenvolver o seu negócio, comunicar e estabelecer relações segmentadas com os clientes. A recolha exponencial de Dados Pessoais aumentou a perceção sobre as preferências e os comportamentos individuais dos consumidores e criou oportunidades de negócio para as empresas que procuram determinadas vantagens competitivas assentes na segmentação e na qualidade de serviço. A Microsoft, por exemplo, utiliza um *software* denominado "*Titan* para processar dados de três das suas fontes - o *LinkedIn*, o *Office 365* e o *Bing*..."[3]. Estas empresas utilizam os Dados Pessoais recolhidos para enriquecer os seus produtos e os seus serviços, acrescentando-lhes valor, reduzindo os ciclos de vida e os períodos de desenvolvimento, mas os Dados Pessoais ajudam também a prevenir fraudes e incumprimentos ao nível dos pagamentos, a recrutar e a selecionar funcionários, ou podem, no limite, simplesmente, ser revendidos a terceiros[4].

A indústria hoteleira é uma atividade económica altamente competitiva e extremamente personalizada. Esta personalização assenta, em grande medida, na informação pessoal recolhida junto dos clientes e na forma de a utilizar para segmentar e otimizar a oferta, contribuindo para a tomada de decisão dos diretores, dos administradores e dos proprietários.

---

[3] PricewaterhouseCoopers (2018). "Using Personal Data to Build Customer Trust and Competitive Advantage. Consultado em maio 3, 2018 em http://pwc.blogs.com/analytics_means_business/2017/02/using-personal-data-to-build-customer-trust-and-competitive-advantage.html

[4] PricewaterhouseCoopers (2018). "Using Personal Data to Build Customer Trust and Competitive Advantage. Consultado em maio 3, 2018 em http://pwc.blogs.com/analytics_means_business/2017/02/using-personal-data-to-build-customer-trust-and-competitive-advantage.html

Vivemos numa sociedade de informação em que são recolhidos, processados e eliminados cada vez mais Dados Pessoais e onde as empresas e autoridades públicas tendem a saber cada vez mais sobre os padrões de comportamento, os hábitos e as preferências dos clientes e potenciais clientes, por vezes, mesmo antes dos próprios. Mas à medida que as oportunidades e os fins de utilização de Dados Pessoais crescem, aumenta também o risco e a necessidade de as empresas protegerem e utilizarem adequadamente as informações armazenadas.

Neste sentido, o preâmbulo do Regime Geral Proteção de Dados refere que "a rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de Dados Pessoais. A recolha e a partilha de Dados Pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de Dados Pessoais numa escala sem precedentes no exercício das suas atividades. Os particulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social contribuíram para facilitar a livre circulação de Dados Pessoais na União e a sua transferência para países terceiros (...)"[6].

Os novos modelos de agregação de informação com recurso a técnicas e tecnologias cada vez mais intrusivas, difusas e camufladas levantam muitas questões, sobretudo, ao nível do que chamamos de Direito à Privacidade.

Como ensina o Professor Oliveira Ascensão (2002)[7] o conceito de privacidade assume entre nós duas formas. A primeira diz respeito a um conceito de origem anglo-saxónica – *privacy* – que se refere a um conjunto de elementos reservados exclusivamente a um individuo e inserido numa visão individualista do Estado e da vida em sociedade". Numa segunda aceção, de base europeia, o Direito à Privacidade é um direito que protege o indivíduo, em conjunto com outros direitos que limitam o poder do Estado e das autoridades públicas sobre a esfera da vida privada dos indivíduos. Este entendimento ganhou os "contornos atuais no período do Iluminismo" [8]. Os artigos 10.º e seguintes do Pacto Internacional dos Direitos Civis e Políticos[9], definem a intenção de proteger as várias dimensões da determinação e da exteriorização da personalidade humana. Estas

[6] Parágrafo 6.º do preambulo do Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[7] Oliveira Ascensão (2002). A reserva da intimidade da vida priva e familiar. In Revista da Faculdade de Direito da Universidade de Lisboa (Vol. XLIII-Nº1, p. 14). Lisboa: Coimbra Editora.

[8] Correia, V. (2014). Sobre Direito à Privacidade. In Miranda, J. O Direito (240 p). Lisboa: Editora Almedina.

[9] Pacto Internacional sobre os Direitos Civis e Políticos e Protocolos Facultativos. In Bacelar Gouveia, J. (2009). *Direito Internacional Público - Textos Fundamentais*. Editora: Coimbra

diferentes dimensões abrandem o Direito à Identidade (nome, aparência, género, religião, etc.), o Direito à Integridade e à Intimidade (domicílio, correspondência e proteção de dados), o Direito à Autonomia (e consequente realização pessoal), o Direito à Comunicação e Direito à Sexualidade. É dentro da esfera do Direito à Privacidade que encontramos o regime de Proteção de Dados Pessoais.

O objetivo do regime de Proteção da Dados Pessoais passa por colocar o indivíduo no centro protegendo-o das violações da privacidade do seus Dados Pessoais e atribuindo-lhes "efetivos direitos (…) reconhecidos constitucionalmente"[10], nomeadamente, através da proibição do uso e da publicação, sem consentimento prévio, das suas especificidades pessoais.

O conflito entre a importância dos Dados Pessoais para as atividades económicas e do Direito à Privacidade tenderá certamente a crescer nos próximos anos, especialmente, em sectores económicos onde são desenvolvidos, em ecossistemas de constante inovação tecnológica, produtos com grande capacidade de recolher Dados Pessoais de utilizadores, como por exemplo, as aplicações informáticas, os dispositivos de comunicação móvel e outros dispositivos eletrónicos que integrem a chamada "internet das coisas".

Desde a década de 1970 que o avanço tecnológico "despertou nos legisladores dos Estados onde a realidade informática se encontrava mais desenvolvida a necessidade de aprovar legislação dotando os indivíduos e as autoridades independentes" [11] dos meios e das ferramentas adequadas para combater os abusos que pudessem ser provocados pelos poderes público ou pelo sector privado[12]. Atualmente, o grande desafio está na adaptação do Estado Social à realidade das tecnologias da informação e à existência de "entidades privadas detentoras de enormes quantidades de dados"[13].

A necessidade de endereçar estes desafios, de estabelecer regras atualizadas relativamente à proteção de Dados Pessoais[14] e de garantir uma harmonização

[10] Mayer-Schonberg, V. (2001). General Development of Data Protection in Europe, in AGRE, Philip E. e Rotenberg, Marc – Technology and Privacy: The New Landscape. Londres e Massachussetts: MIT Press.

[11] Bennett, Colin J. (1992). Regulating Privacy. Data Protection and Public Policy in Europe and the United State. Ithaca: Cornell University Press.

[12] Hespanha, P. (2000). Entre o estado e o mercado. As fragilidades das instituições de proteção social em Portugal. Coimbra: Quarteto

[13] Pinheiro, A. S. (2015). Privacidade e proteção de Dados Pessoais: a construção dogmática do direito à identidade informacional. Lisboa: AAFDL

[14]Nos termos do Artigo 1.o n. º1 e 2 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

legislativa entre os Estados Membros conduziu à revisão das regras de proteção de Dados Pessoais na União Europeia e à mudança do um modelo de proteção externa para um modelo de responsabilidade.

2.2. Regulamento Geral de Proteção de Dados

A 27 de abril de 2016 o Parlamento Europeu aprovou um novo Regulamento Geral de Proteção de Dados (RGPD). O RGPD aplica-se ao tratamento de Dados Pessoais por meios total ou parcialmente automatizados bem como ao tratamento de dados por meios não automatizados contidos em ficheiros ou a eles destinados[16].

O novo Regulamento Geral Proteção de Dados representa uma mudança de paradigma no modelo de regulação do tratamento de Dados Pessoais. Entre outras alterações, que abordaremos adiante, o RGPD consubstancia a passagem de um modelo de hétero-regulação tipicamente imposto por uma organização administrativa independente com poderes de autoridade - no caso português, a Comissão Nacional de Proteção de Dados [17] -, para um modelo de autorregulação.

Nos modelos de autorregulação, cabe às empresas assegurar o cumprimento das regras e evidencia-lo perante uma entidade fiscalizadora. Nos termos do RGPD a prestação de contas – *accountability* – implica a implementação ativa de medidas pelos responsáveis de tratamento de forma a promover e salvaguardar a proteção dos Dados Pessoais, e a manutenção de registos e de documentação previamente preparada para demonstrar a conformidade junto do público e perante as autoridades de publicas de supervisão.

Para além destas alterações, o Regulamento introduz a todos os Estados Membros, a figura do Encarregado de Proteção de Dados (DPO), uma entidade de proteção da privacidade anteriormente existente no Direito Alemão.

---

[16]Nos termos do Artigo 2.o n. º1 e 2 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[17]A Comissão Nacional de Proteção de Dados tem como atribuição "controlar e fiscalizar o processamento de Dados Pessoais", em respeito pelos direitos e liberdades consagradas na Constituição e na Lei. No espaço comunitário, a CNPD coopera com as "autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro" *in* Portal do Cidadão. A CNPD. Disponível em https://www.portaldocidadao.pt/web/comissao-nacional-de-protecao-de-dados/comissao-nacional-de-protecao-de-dados

O RGPD visa garantir o controlo da privacidade dos Dados Pessoais numa sociedade de informação onde a crescente adoção da internet, das redes sociais e de modelos de negócio digitais criam nas pessoas uma predisposição à partilha de informações da sua vida pessoal, muitas vezes sem consideração pelos potenciais efeitos futuros indesejados desenhando um conjunto de regras projetadas para apoiar as empresas no uso de Dados Pessoais, dar aos consumidores a confiança de os dados estarem protegidos e de que, os que deles abusarem serem responsabilizados. Perante este facto, passou também a ser obrigatório a obtenção do consentimento dos titulares no uso dos dados para determinadas finalidades de tratamento, assim como, o seu registo estruturado, podendo o titular dos dados limitar ou opor-se ao tratamento dos dados a qualquer momento.

O Regulamento teve aplicação obrigatória a 25 de maio de 2018 em todos os Estados Membros da União Europeia e substituiu em Portugal a Lei 67/98 que transpôs para a ordem jurídica portuguesa a Diretiva 95/446/CCE.

O primeiro texto constitucional europeu a prever um regime de proteção dos Dados Pessoais foi Constituição da República Portuguesa de 1976[18]. Posteriormente, a 27 de abril de 1991, entrou em vigor a Lei n.º 10/91, "Lei da Proteção de Dados Pessoais face à Informática", que veio regular esta matéria em harmonia com a Constituição. Em 24 de outubro de 1995 a diretiva n.º 95/46/CE31 do Parlamento Europeu e do Conselho definiu os princípios da adequação, da finalidade e da retificação dos dados que foram transpostos em outubro de 1998 pela Lei n.º 67/98 para Portugal. Paralelamente, no plano transatlântico, foi aprovada a Decisão 2000/520/CE32, de 26 de julho, nos termos da Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, conhecida como *Safe Harbor Agreement,* que constituiu um acordo para a compatibilização do modelo legislativo europeu e o modelo de pendor obrigacional (ou contratual) vigente nos Estados Unidos da América. Com a entrada em vigor do Tratado de Lisboa em dezembro de 2009, estabeleceu-se (no seu artigo 16.º do TFUE) que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito (…)".

O RGPD é uma lei extremamente abrangente que impõe regras não só em todos os países da União Europeia, como a todas as empresas que fora do espaço europeu tratem Dados Pessoais de cidadãos europeus [19] [20]. Em alguns casos, o incumprimento das

[18]Artigo 35º da Constituição da República Portuguesa

[19]Não abrange o tratamento de Dados Pessoais relativos a pessoas coletivas.

[20]Artigo 3º do Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016 e parágrafo 14.º do preâmbulo do Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

regras definidas pelo RGPD está sujeito a coimas que podem ir até 20 milhões de Euros ou até 4 % do seu volume de negócios anual a nível mundial consoante o montante mais elevado[21].

As unidades hoteleiras são pela natureza da sua atividade comercial - elevada rotação de clientes, pessoal e inventários - grandes agregadores de Dados Pessoais. As pessoas são a força vital da indústria hoteleira, como refere Paul Greenberg[22], "para além dos principais serviços, da satisfação do cliente assente numa abordagem amigável e em relações interpessoais eficazes, da resolução de problemas e da flexibilidade das opções, os colaboradores, oferecem ao hotel uma vantagem competitiva face aos concorrentes". Conscientes deste facto, a generalidade dos hoteleiros procede a recolha de Dados Pessoais relevantes e pertinentes de forma a acomodar e personalizar as prestações de serviços e as características individuais de cada cliente e de cada colaborador.

2.3. Tratamento de Dados Pessoais

São Dados Pessoais qualquer informação relativa a uma pessoa que, por si só, ou conjugada com outras, a permitam identificar.

Nos termos do artigo 4º 1) do RGPD, "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"[23].

Para além dos exemplos referidos no artigo 4º do RGPD, têm sido considerados como Dados Pessoais pela jurisprudência, quando permitam identificar uma pessoa, o número de cartão de crédito, a data de nascimento, as classificações escolares, o *curriculum vitae*, a história clínica, as dívidas de créditos, os históricos de compras, os históricos dos meios de pagamento, o endereço de I.P. (ou *Internet Protocol Address*), e as publicações em redes sociais[24].

---

[21]Artigo 83º n.º 6 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[22]Greenberg P. (2001). RM at the Speed of Light. Londres: Addison-Wesley Professional.

[23]Artigo 4º 1) Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[24]Tribunal de Justiça da União Europeia. *Processo n.º C-73/07*. Consultado em 12 dezembro 2017 em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd52ff4da201ef4b0d8c7a8875e96eb2f7.e34KaxiLc3qMb40Rch0SaxuQa310?text=&docid=76075&pageIndex=0&doclang=PT&mode=lst&dir=&occ =first&part=1&cid=666398

O regulamento distingue, por exclusão de partes, aquilo a que podemos chamar de dados comuns, dos dados que à luz do artigo 9.º do RGPD são considerados dados sensíveis. Nos termos deste artigo são considerados Dados Pessoais sensíveis aqueles que "revelem a origem racial ou étnica, as opiniões políticas do titular, as suas convicções religiosas ou filosóficas, a filiação sindical, os dados genéticos", os "dados biométricos que permitam identificar uma pessoa de forma inequívoca, dados relativos à saúde, ou dados relativos à vida sexual ou orientação sexual de uma pessoa".

Todas as categorias de Dados Pessoais estão sujeitas à proteção do Regulamento. Nos termos do artigo 4.º 2) do RGPD, tratar um dado pessoal é qualquer "operação ou um conjunto de operações efetuadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição"[25] [26].

Os níveis de exigência para a recolha e tratamento de Dados Pessoais variam em função do tipo de dado pessoal em causa.

Nos termos do artigo 9.º do Regulamento, é proibido o tratamento de Dados Pessoais sensíveis, exceto quando:

- o titular dos dados tiver dado o seu consentimento explícito para uma ou mais finalidades específicas, se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular;

- Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular;

[25]Artigo 4º n.º2 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[26]Em determinadas categorias especiais de dados, como, os Dados Pessoais relacionados com condenações penais, infrações ou medidas de segurança, o tratamento só é permitido sob o controlo de uma autoridade pública ou se autorizado por lei No requerimento de certificado do registo criminal deve ser claramente mencionado o fim a que se destina o certificado do registo criminal por exemplo, se para constituição de sociedade financeira (no caso dos administradores ou proprietários de cadeias hoteleiras que as tenham), ou, se para o exercício de atividade de segurança privada (no caso dos seguranças) (n.º1 do art.º 21.º, n.º2 do art.º 22.º, n.º1 do art.º 24.º do Dec. Lei n.º171/2015, de 25/8).

- o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos;

- o tratamento se referir a Dados Pessoais que tenham sido manifestamente tornados públicos pelo seu titular;

- o tratamento for necessário à declaração, num processo judicial, se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro;

- o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado;

- o tratamento for necessário por motivos de interesse público no domínio da saúde pública, ou;

- o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º n.º 1 do Regulamento.

Às pessoas singulares ou coletivas que determinam as finalidades e os meios de tratamento de Dados Pessoais o RGPD chama de "responsáveis pelo tratamento"[27]. No sector hoteleiro o responsável pelo tratamento será, em princípio, a sociedade comercial detentora da operação e que determina a recolha de dados dos clientes e dos colaboradores, ou eventualmente, a sociedade gestora de participações sociais que controla um determinado grupo empresarial e que partilha os Dados Pessoais dos clientes dentro da esfera das empresas por si detidas.

Nos termos do artigo 25.º do RGPD, cabe ao responsável pelo tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os titulares, definir e aplicar as medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento é realizado em conformidade com o Regulamento.

Para além do "responsável pelo tratamento", são também corresponsáveis pelos danos causados por violação ou uso indevido, na medida das suas responsabilidades, outras

[27]Artigo 4.o n. º7 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

empresas que sejam subcontratadas para os tratar. Um exemplo de serviço de subcontratação, são as empresas de processamento de correio eletrónico ou mensagens de texto em larga escala, contratadas especificamente para este efeito a quem o hotel cede os contactos dos seus clientes[28].

Nos termos do artigo 5.º do Regulamento, no decorrer dos processos de tratamento o responsável pelo tratamento deve respeitar um conjunto de princípios.

Em primeiro lugar os dados devem ser tratados de uma forma lícita, leal e transparente. Nos termos do art.º 6 do RGPD é lícito recolher Dados Pessoais quando:

- O tratamento for necessário para a execução de um contrato no qual o titular dos dados (cliente ou colaborador) é parte, ou para diligências pré-contratuais a pedido do titular dos dados (art.º 6.º b), por exemplo, recolha de dados de clientes para realização de contratos de hospedagem, reservas, pré-reservas e pedidos de orçamento, Dados Pessoais para execução de contratos de trabalho e de interessados envolvidos em processos de recrutamento, ou a recolha de Dados Pessoais de colaboradores de fornecedores para a celebração de contratos de fornecimentos de bens e de serviços, etc.;

- O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o hoteleiro esteja sujeito (art.º 6. c). Relativamente ao Imposto sobre o Rendimento de pessoas Coletivas (IRC), a Lei n.º 2/2014 de 16/01 refere que os registos contabilísticos e documentos de suporte devem ser "conservados em boa ordem" durante o prazo de 12 anos[29], alterando o prazo anterior de 10 anos; relativamente ao imposto sobre o valor acrescentado (IVA) os registos contabilísticos e os documentos de suporte devem ser arquivados e conservados durante 10 anos; relativamente a imóveis as faturas das obras devem ser guardadas pelo período mínimo de cinco anos, tal como os recibos da renda da casa e os comprovativos de pagamento das quotas de condomínio. No caso dos hotéis é obrigatória a recolha de Dados Pessoais para preenchimento de boletins de alojamento, que se destinam a permitir o controlo dos cidadãos estrangeiros e posterior comunicação ao Serviço de Estrangeiros e Fronteiras (ou nas localidades onde este não exista, à Guarda Nacional Republicana ou à Polícia de Segurança Pública,) nos termos do artigo 15.º da Lei n.º 23/2007, de 4 de julho;

[28]A este respeito uma nota adicional: o RGPD define «subcontratante» como "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os Dados Pessoais por conta do responsável pelo tratamento destes" (art.º 4. n. º8 RGPD). Esta definição parece ser um manifesto lapso de tradução, uma vez que, o que se encontra definido é o conceito de "subcontratado" e não de "subcontratante" que são a definição e o definido que respeitam o espirito da lei. A correção será feita, certamente, aquando da transposição da norma para o direito português.

[29]Artigo 123.º Lei n.º 2/2014 de 16/01

- O titular dos dados tiver dado o seu consentimento para uma ou mais finalidades específicas[30]. As situações mais comuns que fazem depender de consentimento na atividade hoteleira serão os programas de fidelização de clientes, os registos de utilizadores em *website* da internet, o controle da qualidade de serviço através de inquéritos de satisfação e a comunicações para efeitos de marketing e promoção, etc.

Para além destes casos, o regulamento enumera ainda três outras situações gerais de licitude de tratamento[31]: quando o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; quando, o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; ou, quando, o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais, em especial se o titular for um menor.

Quando o tratamento é realizado com base no consentimento, o "responsável pelo tratamento" deve poder demonstrar por via de evidência, que o titular dos dados deu o seu consentimento para o tratamento dos seus Dados Pessoais. Este consentimento deve ser tão fácil de retirar quanto de dar e no texto informativo a facultar, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente de outros assuntos de "modo inteligível e de fácil acesso e em linguagem clara e simples"[32]. Se no respetivo texto de consentimento existirem termos que constituam violação do regulamento, os mesmos não são vinculativos para o titular do texto que consente[33].

De referir ainda que o titular dos dados tem o direito de retirar o seu consentimento a todo o momento não comprometendo a licitude do tratamento efetuado com base no consentimento até esse momento. Esta informação deve constar do próprio texto do consentimento, uma vez que é o próprio RGPD, no artigo 7.º, que impõe a necessidade de informar o titular desse facto na recolha.

Ao avaliar se o consentimento é dado livremente há que verificar com a máxima atenção se, a execução do contrato está subordinada ao consentimento para o tratamento de Dados Pessoais que não é necessário para a execução desse contrato. Por outro lado,

[30] Artigo 4.º n. º2 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[31] Artigo 6.o n. º1 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[32] Artigo 7.o n. º1 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[33] Artigo 7.o n. º2 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

quando existir necessidade de consentimento e o titular em causa tenha menos de 16 anos, “o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança”[34].

Os Dados Pessoais fornecidos no ato da recolha são em princípio prestados por escrito ou por meios eletrónicos. Se o titular dos dados o solicitar, esta informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios [35].

Os Dados Pessoais recolhidos para tratamento devem ser aqueles que sejam considerados adequados, relevantes e limitados ao mínimo necessário para cumprir as finalidades de tratamento[36] [37]. De acordo com o art.º 6 do RGPD, os Dados Pessoais têm de ser recolhidos para finalidades determinadas e explícitas (como por exemplo, gestão económica, contabilística, fiscal, gestão de faturação, gestão de clientes, gestão de reservas, histórico de relações comerciais, gestão de cobranças e pagamentos, marketing, fidelização de clientes, registo de utilizadores em site da internet, controle da qualidade de serviço, gestão de fornecedores ou gestão de recursos humanos[38]) não podendo serem tratados posteriormente de uma forma incompatível com as finalidades para os quais foram recolhidos.

Por exemplo, no ato de uma reserva de alojamento o hoteleiro não necessita de pedir consentimento para tratar os Dados Pessoais dos clientes (nomes, contactos, dados faturação, etc.,) necessários para efetuar a reserva, mas estes dados não podem posteriormente ser utilizados para fins de marketing ou comunicação, uma vez que esta finalidade é distinta daquela que justificou a recolha original dos dados. A comunicação e a promoção são essenciais ao negócio hoteleiro, uma estratégia aconselhável para proceder ao uso dos dados recolhidos nas reservas, pode passar por recolher um consentimento adicional para efeitos de marketing (SMS e e-mail) na confirmação da reserva.

No âmbito da nova lei é licito as empresas definirem perfis de forma automatizada, processando informações pessoais de uma forma informatizada, sem ação humana, com o objetivo de avaliar e tipificar os clientes com base nos seus Dados Pessoais. Mas com o RGPD os consumidores passam a ter o direito de não ficar sujeitos a nenhuma “decisão

[34] Artigo 8.o n. º1 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[35] Artigo 12 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[36] Artigo 5.º b) Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[37] Artigo 5.º c) Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[38] Como resulta do formulário de notificação de tratamento à CNPD disponível em https://www.cnpd.pt/bin/Duvidas/geral.aspx

tomada exclusivamente com base no tratamento automatizado, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar" [43].

No sector hoteleiro, é tecnicamente possível atribuir tarifas diferentes para os mesmos serviços em função da origem do cliente ou da localização no momento da consulta da disponibilidade e da tarifa. É o que acontece no caso dos agregadores *online*, quando um determinado cliente que faz uma pesquisa a menos de *x* quilómetros do hotel *y* recebe uma proposta com tarifa diferente de outro cliente que faz consulta igual em lugar mais próximo ou distante. Neste caso, o sistema informático utiliza Dados Pessoais de geolocalização para criar um perfil e modifica o comportamento para que, através de segmentação, oferecer a clientes em localizações diferentes, tarifas diferentes. Com o RGPD os clientes têm de ser informados desta possibilidade caso exista este tipo de tratamento podendo assim impedir que os seus dados sejam processados desta forma ou pôr em causa a decisão daí decorrente.

Outros tipos de definição de perfis permitem que clientes com níveis predefinidos de fidelização ou de consumo tenham acesso a produtos ou preços específicos. É o que acontece no caso das *online travel agencies* que fazem depender a apresentação de determinados preços especiais de um *login* prévio, tornando assim a definição de perfis uma condição de utilização das suas aplicações, isto é, o *login* é parte integrante do produto o que contorna a possibilidade de oposição às decisões. Noutros casos, os responsáveis pelo tratamento (*online travel agencies* e hotéis) poderão solicitar o consentimento explícito para definir perfis e executá-los quando essa definição seja relevante, como por exemplo, para a distribuição dos produtos.

Relativamente ao tratamento de Dados Pessoais sensíveis, importa salientar que a recolha tenderá a verificar-se em maior número aquando dos processos de recrutamento pelo que o hoteleiro deverá excluir, logo à partida, alguns desses dados da recolha, como os dados que revelem a origem racial ou étnica, as opiniões politicas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos e os dados relativos à vida sexual ou orientação sexual de uma pessoa. No caso dos dados biométricos – assinaturas e impressões digitais - que permitem identificar uma pessoa de forma inequívoca, estes tendem cada vez mais a ser utilizados como elemento da relação de trabalho e como forma de controlo dos tempos de trabalho e picagens de ponto[44]. Poderá ainda levantar-se a hipótese de determinados dados, como o número de quarto, a data de estadia, e pedidos de *room service*, quando conjugados, constituírem

[43] Artigo 22.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[44] Artigo 9.º 1) Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

categorias especiais, uma vez que, permitem em determinados casos identificar a dieta ou saúde alimentar de um cliente. Estas e outras questões necessitarão de clarificação jurisprudencial.

Durante o processo de tratamento dos dados, cabe ao hoteleiro demonstrar a conformidade com o RGPD e verificar, obrigatoriamente, a relevância e razoabilidade de guardar e tratar os Dados Pessoais recolhidos.

O Regulamento impõe a responsabilidade de tratar os dados de forma a garantir a segurança, incluindo a proteção contra tratamento não autorizado ou ilegal, perdas, destruições ou danos acidentais, utilizando as medidas técnicas ou organizacionais adequadas.

Nos termos do artigo 30.º do Regulamento, as empresas com pelo menos 250 trabalhadores devem manter um registo escrito que permita identificar o nome e os contactos do responsável pelo tratamento, as finalidades do tratamento dos dados, a descrição das categorias de titulares de dados e das categorias de Dados Pessoais, as categorias de destinatários a quem os Dados Pessoais foram ou serão divulgados, as transferências de Dados Pessoais para países terceiros, a documentação que comprova a existência das garantias adequadas e, se possível, os prazos previstos para o apagamento das diferentes categorias de dados e uma descrição geral das medidas técnicas e organizativas no domínio da segurança[45]. O hotel deverá manter esta informação em registo comum e por um período não superior ao necessário para as finalidades para as quais os dados são recolhidos. Estes deveres são extensíveis aos subcontratantes, nos termos n.º 2 do mesmo artigo.

Por outro lado, os titulares dos dados adquirem direitos definidos, que incluem: o direito à transparência da informação, o direito de acesso e retificação; o direito ao processamento restringido; o direito à portabilidade dos dados; o direito de objetar; e o direito ao apagamento [46]. Desta forma, o RGPD impõe aos hotéis o desenho de processos para responder aos pedidos de acesso dos titulares para corrigir e apagar os Dados Pessoais, para limitar tratamentos para fins de marketing direto, para solicitar a revisão manual de decisões automáticas, para notificar a Autoridade Supervisora em

[45] Artigo 30º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[46] É neste contexto que as novas regras de proteção de dados desenvolveram o "Direito ao Esquecimento", que se consubstancia no direito dos utilizadores em solicitar que os seus dados sejam apagados forçando, entre outros, "os gigantes das redes sociais a excluírem *posts*" indesejados. Brown R., (2017, 7 Agosto). UK consumers will be able to force social media giants to delete embarrassing posts under new data law. Consultado em janeiro 15, 2018 em https://www.cnbc.com/2017/08/07/uk-consumers-to-have-right-to-be-forgotten-under-data-protection-law.html

caso de violação, para retirar o consentimento para determinado tratamento e para solicitar portabilidade dos dados quando esta seja tecnicamente viável.

É importante que os colaboradores e os terceiros subcontratados possam rapidamente enquadrar todas estas situações em conjunto com os direitos dos titulares dos dados. Por isso, nas unidades hoteleiras e nos departamentos centrais que tratam Dados Pessoais deverão existir instruções claras para a manipulação dos pedidos dos titulares dos dados, e manuais de normas definidos e implementados de modo a garantir consistência, previsibilidade e responsabilidade. Para além disto, devem ser oferecidas ações de formação e sensibilização no âmbito da privacidade e da proteção de Dados Pessoais a todos os colaboradores.

Também no sentido de garantir os direitos dos clientes devem ser revistos os contratos com os terceiros contratados para tratar os dados, de modo a coordenar com eles as medidas necessárias e a inclusão de cláusulas contratuais que garantam a conformidade com o RGPD por todas as partes.

Do ponto de vista técnico, as infraestruturas informáticas dos hotéis deverão ser suficientemente robustas para garantir a qualidade dos dados e a deteção de violações, internas ou externas, e tomar as medidas apropriadas para recuperação dos dados e a continuidade do negócio. Para todas as atividades de tratamento os responsáveis hoteleiros devem avaliar os riscos associados, particularmente no caso de dados de categorias especiais e tomar as medidas adequadas de proteção e mitigação dos riscos, nomeadamente, no desenvolvimento de novos sistemas e procedimentos com a componente adicional da análise do impacto em termos de privacidade e de proteção dos Dados Pessoais.

O agravamento das sanções, que podem ir até vinte milhões de euros ou 4% do volume de negócios global são, por si só, razão suficiente para colocar este tema na agenda das administrações e direções dos grupos hoteleiros e suscitar a necessidade da correta implementação. Contudo, o nível de exigência e a complexidade do tema do Regulamento Geral de Proteção de Dados coloca desafios complexos à mudança dos processos na generalidade das empresas.

2.1. Implementação do Regulamento Geral de Proteção de Dados

Implementar o Regulamento Geral de Proteção de Dados consume tempo e recursos à operação hoteleira, tem impactos consideráveis nos processos e no desempenho dos sistemas de informação e interfere com as atividades dos diversos departamentos. Ainda

que, confira alguma minimização de processos o RDPG é, basicamente, um centro de custos para as empresas.

As vantagens diretas do RGPD estão na manutenção da idoneidade e em evitar coimas e multas de incumprimento dos requisitos, assim como, evitar eventuais indemnizações por danos causados aos titulares dos dados em caso de fuga ou violação de dados. Por isso, do ponto de vista da gestão, um dos principais objetivos passa por atenuar os impactos da própria implementação.

Implementar uma legislação como o RGPD implica uma sensibilização tanto ao nível dos operacionais como dos diretores e administradores. Num estudo realizado pela KPMG (uma multinacional de auditoria, fiscalidade e consultoria) de março de 2017 [47], um grupo de empresas portuguesas enumeraram como principais desafios no esforço de conformidade das suas operações com o RGPD. Entre as principais dificuldades enumeradas figuraram: a ausência de recursos especializados; as limitações dos sistemas de informação; a multiplicidade das atividades de tratamento e a necessidade de ajustamento dos processos de negócio.

Para além destes, existem ainda outros fatores extremamente desafiantes para as empresas, como sejam: a confiança excessiva na formação e na capacidade de mudança; as questões relativas aos direitos de portabilidade e da sua implementação; a atualização dos avisos de privacidade e de marketing; as notificações às autoridades em caso de violação de dados; a análise dos contratos com terceiros que tratem os dados por conta dos responsáveis; os processos relativos ao direito ao esquecimento; a criação de um inventário dos dados e de tratamentos; o desenvolvimento de um ecossistema tecnológico que permita identificar os impactos que os requisitos de GDPR; e a implementação de um plano de correção para adequar as conformidades com o GDPR numa escala corporativa.[48].

De forma a colmatar os efeitos negativos nos processos nas empresas, a União Europeia definiu um prazo legal entre a publicação e o início da vigência do Regulamento – *vacatio legis* – de dois anos, ou seja, entre maio de 2016 e maio de 2018 as empresas tiveram oportunidade de implementar as medidas que julgaram necessárias para endereçar as exigências deste novo modelo de tratamento de Dados Pessoais.

[47] "O Impacto do Regulamento Geral de Proteção de Dados em Portugal, Estudo, março 2017, kpmg.pt

[48] De Bos, T. (2018), GDPR Today & Tomorrow, how to create a sustainable GDPR implementation? Consultado em maio 15, 2018 em https://consulting.ey.com/ready-eus-new-general-data-protection-regulation/

De uma forma geral, as empresas viram-se obrigadas a desenvolver e melhorar os processos de tratamentos de Dados Pessoais, tanto ao nível de dados internos (referentes a trabalhadores e outros prestadores de serviços), como de Dados Pessoais de indivíduos externos à organização (clientes e potenciais clientes).

Os processos de negócio tiveram também de ser adaptados para dar resposta às necessidades de cada tipo de tratamento e às exigências transversais a todos, como a aplicação de proteção de dados desde a conceção e por defeito nos seus produtos e serviços - *privacy by design and default*- a comunicação ao titular de toda a informação obrigatória aquando da recolha de Dados Pessoais, ou o registo das evidências do consentimento explícito prestado pelos titulares dos dados para o tratamento dos seus Dados Pessoais, quando necessário.

Por um lado, existe uma tendência cada vez maior em adotar tratamentos de dados inovadores e sofisticados, compostos por modelos analíticos de perfis de consumo, dados de geolocalização ou redes sociais para potenciar o negócio. Mas por outro lado, em muitas empresas, os sistemas de informação apresentam diversas limitações e deficiências ao nível das autorizações de acesso ou do registo de acesso a categorias especiais de dados. Com o Regulamento Geral de Proteção de Dados estas limitações podem ficar mais evidentes.

No momento da escolha do hotel, o hóspede tem a expectativa de se sentir bem-recebido, respeitado e seguro. Estas preocupações com o serviço ao cliente devem estender-se, também, à forma como os seus Dados Pessoais e a sua privacidade são tratados e respeitados

Como ponto de partida, as organizações devem avaliar, face ao volume, categorias, sensibilidade e duração do tratamento, a necessidade de contratar um Encarregado de Proteção dos Dados (*Data Protection Officer* ou DPO).

Nos termos do artigo 37.º do RGPD os responsáveis pelo tratamento e os subcontratantes devem designar um encarregado da proteção de dados sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala, ou sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados.

O Encarregado da Proteção de Dados é designado com base nas suas qualidades profissionais e, em especial, e nos seus conhecimentos especializados no domínio do Direito e das práticas de proteção de dados. Nos termos do artigo 37.º do RGPD, um grupo empresarial, como uma cadeia hoteleira, pode designar um único encarregado da proteção de dados desde que haja um encarregado da proteção de dados que seja facilmente acessível a partir de cada estabelecimento.

A existência de um Encarregado de Proteção dos Dados implica a criação de um modelo de articulação com a organização, o desenvolvimento de um perfil das competências técnicas e competências funcionais do cargo. Cumulativamente, é necessário definir um posicionamento orgânico do DPO no seio da empresa que garanta que a função é exercida de uma forma independente, sem conflitos de interesses e com autoridade. O DPO depende de um modelo de gestão que fomente a responsabilidade de todos os órgãos relevantes no tratamento dos Dados Pessoais. Esta abordagem facilita a manutenção de uma cultura de proteção de Dados Pessoais no seio do hotel. O hoteleiro deverá ainda publicar os contactos do encarregado da proteção de dados e comunicá-los à autoridade de controlo.

O encarregado da proteção de dados tem as seguintes funções: informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações; controlar a conformidade com o regulamento, e com outras disposições relativas à proteção de Dados Pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização; cooperar com a autoridade de controlo; e ser o ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º do Regulamento[50].

O regime do Regulamento Geral de Proteção de Dados tem como principal objetivo controlar a perda de Dados Pessoais e atenuar os danos para os particulares e para o hotel em caso de violação. Para além dos ataques informáticos ao sistema, uma percentagem significativa dos incidentes ocorridos nas organizações tem origem interna e resulta de erro humano, de desconhecimento ou de má aplicação de princípios internos. De forma a atenuar estes riscos, as organizações devem definir programas de

[50] Nos termos dos Artigo 39º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

sensibilização e formação em matéria de proteção de dados, ações de formação direcionadas para categorias de utilizadores específicas, exercícios de sensibilização direcionados para a generalidade dos colaboradores e divulgar os comportamentos adequados a ter durante e após o fim do contrato.

Outro requisito é a criação de um Código de Conduta e de uma Política de Privacidade descrevendo os processos e os procedimentos que regulam todos os tratamentos de Dados Pessoais nos termos do RGPD e que estabeleçam quais as boas práticas a ter pelos funcionários. Devem também ter-se em linha de conta as questões relativas ao uso das contas de *e-mail* e dos sistemas de gestão integrados.

O Regulamento Geral de Proteção de Dados menciona a necessidade da existência de um Código de Conduta para facilitar a sua correta aplicação. A elaboração e adoção de uma Política de Privacidade tem um cariz público e revela as opções da empresa e os princípios que lhe estão subjacentes e que devem ser observados pelos colaboradores, sendo um instrumento para demonstração de conformidade [51].

Os hotéis e grupos hoteleiros devem ainda formalizar um conjunto adicional de documentação direcionada a fomentar a correta aplicação das obrigações decorrentes do Regulamento, nomeadamente, a Avaliação de Impacto da Proteção de Dados.

A Avaliação de Impacto da Proteção de Dados (ou, na denominação anglo-saxónica, DPIA, Data *Protection Impact Assessment*) é um documento concebido para descrever o processo de tratamento de Dados Pessoais, averiguar da sua necessidade e proporcionalidade e ajudar a gerir os riscos resultantes do tratamento para os direitos e liberdades dos titulares dos dados[52]. Os resultados desta avaliação são tidos em conta na determinação das medidas tomadas para comprovar que o tratamento de Dados Pessoais está em conformidade com o Regulamento.

Nos termos do artigo 35.º do Regulamento, "quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de Dados Pessoais". Ao efetuar uma avaliação de impacto sobre a

[51] Nos termos dos artigos 5º, 24º e 39º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[52] Nos termos do artigo 35º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

proteção de dados, o responsável pelo tratamento solícita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.

A realização de uma avaliação é obrigatória nos seguintes casos [53]:

- Quando a avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, seja baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

- Quando existam operações de tratamento em grande escala de categorias especiais ou de Dados Pessoais relacionados com condenações penais e informações a que se refere o artigo 10.o; ou c)

- Ou, quando exista o controlo sistemático de zonas acessíveis ao público em grande escala.

Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco para o titular dos dados, um risco que o responsável pelo tratamento não pode atenuar através de medidas adequadas atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de Dados Pessoais.

Os gestores hoteleiros deverão desenvolver estas avaliações sempre que necessário, nomeadamente, quando exista a recolha de dados sensíveis, tanto no âmbito das informações recolhidas para efeitos de reservas, ou prestações de serviço ligadas a serviços conexos em que sejam responsáveis pelo tratamento (serviços de saúde, SPA, etc.).

Outra medida relevante é a definição dos princípios para a contratação de parceiros externos que fazem o tratamento de Dados Pessoais. Nesta matéria, o Regulamento Geral de Proteção de Dados eleva o nível de exigência e define regras para as diferentes etapas do ciclo de vida da relação com as entidades contratadas. É conveniente que as entidades hoteleiras, para além de aferirem da capacidade para tratar os Dados Pessoais, mantenham um inventário das entidades terceiras que têm acesso direto ou indireto aos seus Dados Pessoais e que formalizem instrumentos jurídicos e contratuais para regular as obrigações e os direitos das empresas contratadas.

[53] Nos termos do artigo 35º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

Os danos para o grupo hoteleiro em caso de violação ou más práticas de proteção de dados podem ser significativos. Estes podem consubstanciar-se em perdas financeiras e de receitas por perda de capacidade operacional, perdas de reputação, despesas com notificações a clientes, custas com perícias feitas for investigações e informáticos forenses, custos com indemnizações e responsabilidade civil terceiros ou gastos de defesa. As medidas propostas para cumprir estes requisitos encontram-se descritas no Capítulo 4 deste relatório.

3. Grupo Vila Galé

O Grupo Vila Galé foi fundado em meados dos anos 1980 por Jorge Rebelo de Almeida, José Silvestre Lavrador e José Ruivo, e está entre as 200 maiores empresas hoteleiras do mundo[54]. O grupo Vila Galé é o segundo maior grupo hoteleiro português - o décimo quinto a operar no Brasil, - com vinte e oito hotéis no total, vinte e três em Portugal, sete no Brasil e possui um conjunto de submarcas, das quais destacamos a "Vila Galé Collection", a "Inevitável", a "Satsanga SPA & Health Clubs" e a "Casa Santa Vitória".

Depois da abertura do Hotel Apartamento Vila Galé na praia da Galé o grupo expandiu, primeiro com a abertura do Vila Galé Praia e Vila Galé Cerro Alagoa, em Albufeira e Armação de Pera, respetivamente, Vila Galé Cascais, Vila Galé Ericeira e Vila Galé Porto[55]. Em 2001 a Vila Galé iniciou operações no Brasil com o Hotel Vila Galé Fortaleza. Seguiu-se a abertura do Hotel Rural Vila Galé Clube de Campo em Beja, onde se localizam as vinhas e os olivais do Grupo[56], o Vila Galé Ópera, em Lisboa, o Vila Galé Ericeira e Vila Galé Tavira. Durante o período de 2003 a 2010 o Grupo abriu o "Vila Galé Salvador, o Vila Galé Marés, o Vila Galé Eco Resort do Cabo e o Vila Galé Eco Resort de Angra" [57].

A partir de 2010 foi inaugurado o Hotel Vila Galé Cumbuco, o Vila Galé Santa Cruz na Madeira, o Vila Galé Lagos e o Vila Galé Coimbra. Em 2013 o grupo inaugurou o Vila Galé Collection Palácio dos Arcos, o primeiro da submarca "Vila Galé Collection". Em 2014 foi inaugurado o Hotel Vila Galé Rio de Janeiro, o Vila Galé Évora e o Vila Galé Douro. Em 2017 foi lançada a segunda unidade na cidade do Porto Vila Galé Porto Ribeira. Em abril de 2018 foi aberto o Vila Galé Sintra e lançado projetos em Elvas e Braga e o Vila Galé Touros no Estado brasileiro do Rio Grande do Norte. Para além da notoriedade conquistada com o serviço ao cliente e o controle de custos, a localização tem sido um fator determinante na concretização dos projetos.

Paralelamente, o grupo desenvolveu a marcas de vinhos e de azeite e projetos de agroturismo. O Inevitável é um espaço presente em alguns dos hotéis Vila Galé dirigido à gastronomia. Os SPA Satsanga estão disponíveis em 9 hotéis Vila Galé – Albacora, Praia, Lagos, Coimbra, Santa Cruz, Marés, Eco Resort do Cabo e Eco Resort de Angra e Cumbuco e o Satsanga Health Club, está disponível nos restantes 18 hotéis. A casa

[54] Vila Galé. Media Kit. Disponível em https://www.vilagale.com/pt/grupo/media-kit

[55] Vila Galé. Santa Vitória. Disponível em http://www.santavitoria.pt/pt/empresa/valores.html

[56] Vila Galé. Media Kit. Disponível em https://www.vilagale.com/pt/grupo/media-kit

[57] Vila Galé. Media Kit. Disponível em https://www.vilagale.com/pt/grupo/media-kit

de Santa Vitória fundada em 2002 é uma empresa do grupo Vila Galé centrada na produção e comercialização de vinho e azeite da região do Alentejo, localizada no Vila Galé Clube de Campo[58] .

No total o grupo possui 6438 quartos, 12652 camas e uma equipa de 2300 funcionários. Portugal representa a maior fatia de negócio, onde o grupo tem o maior número de unidades hoteleiras. O Brasil detém o maior número de hotéis com o conceito *de resort all inclusive* em que 90% da ocupação é garantida por brasileiros. Os *resorts* procuram ser um produto diferenciador com unidades maiores, mais áreas de animação e espaços de lazer e uma cultura de serviço.

O Grupo Vila Galé tem um perfil de hotéis alargado – cidade, eventos, lazer, família – que abrange todas as faixas etárias e um conjunto alargado de mercados emissores, sendo os mais proeminentes, Inglaterra, Holanda, Espanha, França e Alemanha. Para além do aumento da notoriedade de Portugal, os problemas com a segurança em alguns dos principais países concorrentes - Egipto, Tunísia, Turquia - são geralmente apontados como uma das principais razões para o crescimento do turismo em Portugal. Atualmente, o grande desafio para os hotéis, passa por capitalizar esse fluxo, procurar índices de satisfação de clientes elevados, fidelizando-os e atenuando os abrandamentos do crescimento nacional quando estes destinos voltarem a recuperar.

A política de preços do Grupo Vila Galé assenta em aumentos consistentes de preço médio através de mudanças nos canais de distribuição ou das próprias tipologias de quartos. Trata-se sobretudo de um esforço de vendas orientado para vender mais suites ou mais quartos vista mar, em vez de quartos *standard*, captando maior negócio para as épocas baixas (entre novembro e março), consolidando a operação nos hotéis mais recentes e desenvolvendo novos conceitos e projetos em carteira.

Em termos nacionais o Grupo Vila Galé procura responder aos desafios do sector reduzindo a sazonalidade, intensificando a promoção do interior do país e o desenvolvimento da oferta turística com alojamento, produtos e animação e apostando em nichos de mercado como o turismo equestre, ecoturismo e o enoturismo, a otimizando a oferta, em particular na época alta, requalificando os recursos humanos e captando novos mercados, onde a China e os EUA poderão ser mercados centrais.

[58] Vila Galé. Media Kit. Disponível em https://www.vilagale.com/pt/grupo/media-kit

Genericamente, os acessos aos *websites* e o *word of mouth* têm-se revelado as principais fontes de pesquisa para os viajantes no momento da decisão do destino e da formalização da compra. Em termos de planeamento de marketing a Vila Galé desenvolveu o seu *website* de forma a conduzir maior informação e conhecimento ao cliente com o objetivo de promover os seus serviços, através de nichos a clientes e potenciais clientes, seguindo a tendência geral de subida de investimento nos dispositivos móveis - *tablet e mobile* - e a correspondente diminuição do investimento nos média tradicionais e de comunicação massiva.

As principais apostas do sector vão no sentido da personalização e desenvolvimento de tecnologia de automatização de processos. Estas técnicas permitem oferecer serviços aos clientes consoante as estadias anteriores, adequar as preferências através de segmentação *online* e da adaptação do *website* corporativo à navegação do cliente e definir promoções de acordo com a análise de bases de dados seja por correio eletrónico, *newsletter* ou mensagem texto.

A utilização dos Dados Pessoais é essencial para a concretização destes modelos de promoção, de comunicação e para a implementação destas estratégias.

3.1. Hotel Vila Galé Ópera

O Hotel Vila Galé Ópera é uma unidade de 4 estrelas inaugurada em julho de 2002 em Lisboa, frente ao Rio Tejo, próximo ao Centro de Congressos de Lisboa.

Figura 1 "Localização do Hotel Vila Galé Ópera" (fonte Google *Maps* 2018)

O Hotel Vila Galé Ópera está orientado para o segmento de "negócios, familiar e temático"[59], com decoração inspirada na música clássica e na ópera. O hotel dispõe de 259 quartos, dos quais 16 são *suites* júnior.

[59] Vila Galé. Media Kit. Disponível em https://www.vilagale.com/pt/grupo/media-kit

O hotel dispõe de cinco espaços para reuniões e banquetes, clube de saúde com piscina interior, academia, sauna, banho turco e salas de massagens, um restaurante e um bar. Os quartos superiores incluem roupão, chinelos, oferta de garagem e de minibar.

Twin Standard	224	Em todos os pisos
Twin Standard Superior	19	Piso 5
Suite Junior	16	Em todos os pisos (2 por piso)

Tabela 2 "Tipologia de Quartos" (Fonte Própria, 2018)

Os pontos fortes do Vila Galé Ópera são o número de quartos, a capacidade para acolher grupos de congresso e de turismo, a sua localização privilegiada e a vista sobre o rio Tejo, a capacidade do parque de estacionamento, quer seja para autocarros de turismo quer viaturas particulares e a proximidade do Centro de Congressos de Lisboa.

Estes pontos fortes, associados às oportunidades registadas com o aumento do número de rotas e de frequência de voos no aeroporto de Lisboa, o aumento do número de eventos internacionais, como a *Web Summit*, a abertura do elevador panorâmico junto ao hotel e a proximidade de edifícios históricos que possibilitam a criação de roteiros turísticos, alavancam as potencialidades desta unidade e a sua relevância dentro do Grupo Vila Galé.

Contudo, não devem ser descurados alguns pontos fracos, como a limitação de capacidade do restaurante para receber os grupos mais alargados que o procuram, o aumento da oferta de mais camas e de alojamento local em Lisboa, o ruído provocado pelos veículos que circulam na Ponte 25 de abril nos quartos da ala nascente a distância ao centro da cidade.

O quadro de funcionários está apresentado no organograma da Tabela 3 podendo verificar que o Diretor Geral é o responsável pelas ações desenroladas no empreendimento ao qual respondem os chefes de departamento.

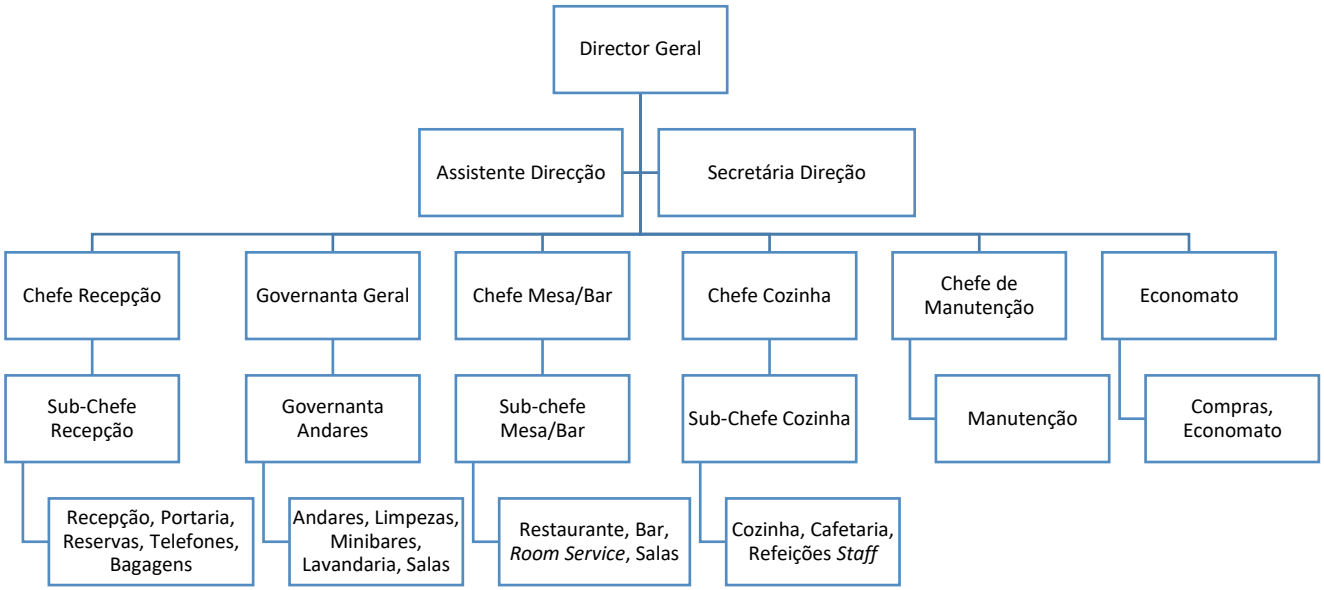

Figura 2 "Organograma Vila Galé Ópera" (Fonte Própria 2018)

4. Tarefas desenvolvidas

Este estágio curricular foi inserido no âmbito do Mestrado em Gestão e Direção Hoteleira da Escola Superior de Turismo e Tecnologia do Mar, do Instituto Politécnico de Leiria, e teve a duração de 10 meses. O estágio decorreu em formato de *cross training* conforme descrito no cronograma constante na Tabela 3.

	set 17	out 17	nov 17	dez 17	jan 18	fev 18	mar 18	abr 18	mai 18	jun 18	jul 18
Departamento de Administração											
Departamento de Marketing											
Departamento de Reservas Individuais											
Departamento de Reservas de Grupos											
Departamento de *Revenue*											
Departamento de Vendas Comerciais											
Departamento de Compras											
Departamento Jurídico											
Departamento de Direção - Vila Galé Opera											

Tabela 3 Cronograma do Estágio por Departamento (Fonte Própria, 2018)

Dentro do âmbito de cada departamento foram desenvolvidas as seguintes tarefas:

	Tarefas desenvolvidas por Departamento
Departamento de Administração	- Participação em reuniões com membros da Administração; - Participação em ação de formação promovida pela S21; - Participação em ação de formação promovida pela Reditus; - Participação na conferência "*Beyond – Portugal Digital Revolutions*", promovido pela EY Portugal, na Fundação Calouste Gulbenkian (17 de outubro de 2017); - Participação na Acão de formação "Regulamento Geral de Proteção de Dados", promovido pela Ordem dos Advogados, Lisboa (3 de maio de 2018); - Participação em reuniões de trabalho com a Microsoft Portugal; - Participação em reuniões de trabalho com especialistas da área da segurança informática da Reditus, SA.
Departamento de Marketing	- Campanha de *Vouchers Presente* e *Vouchers Oferta*; - Apoio à equipa comercial; - Gestão de permutas *Vouchers*; - Desenvolvimento do Manual de Procedimentos ERP.
Departamento de Reservas Individuais	- Gestão de reservas individuais; - Desenvolvimento do Manual de Procedimentos ERP.
Departamento de Reservas Grupos	- Receção de reservas de grupos por correio eletrónico; - Análise de propostas; - *Routing* de grupos; - Desenvolvimento do Manual de Procedimentos ERP;

Departamento de *Revenue Management*	- Análise de taxas de ocupação e de receita das unidades para otimização do preço de venda; - Análise de outras informações estatísticas (pick-up) para definição de preço e disponibilidade; - Análise de comparativos de concorrência; - Desenvolvimento do Manual de Procedimentos ERP.
Departamento Comercial	- Atualização de contratos comerciais; - Acompanhamento em visitas de manutenção; - Participação na Conferência de Marketing e Vendas Vila Galé; - Desenvolvimento do Manual de Procedimentos ERP;
Departamento de Compras	- Acompanhamento de contratos de fornecimento; - Desenvolvimento do Manual de Procedimentos ERP;
Departamento Jurídico	- Reclamação de créditos; - Desenvolvimento de Regulamentos; - Participação em reuniões DRHP;
Departamento de Direção do Hotel Vila Galé Ópera	- Acompanhamento geral da operação do hotel; - Elaboração de ordens de serviço; - Elaboração da previsão semanal; - Controle de horários e escalas; - Visitas de inspeção a quartos e salas; - Análise da taxa de ocupação; - Acompanhamento às salas, serviços, *staff*; - Verificação de relatórios diários na ausência do Diretor; - Vistorias a zonas de clientes e *staff* – iluminação, temperatura, limpeza e arrumação - incluindo terraços áreas circundantes, jardins, salas de reunião; - Recolha de inquéritos a clientes; - Acompanhamento de simulacro de incêndio; - Gestão de placards promocionais internos; - Desenvolvimento de estratégias de dinamização, melhoria constante e redução de custos em todas as áreas; - Acompanhamento da coordenação do HACCP; - Acompanhamento dos procedimentos, cartas, grelhas e custos de F&B; - Conferência de faturas; - Vistoria diária de quartos; - Acompanhamento regular de *tour leaders* e guias com reuniões de trabalho ou refeições; - Contacto com clientes para obtenção do *feedback* das suas experiencias; - Acolhimento pessoal de eventos na unidade, controle das expectativas dos clientes e monitorização constante do *feedback* do organizador; - Controle de Câmbios; - Análise de concorrência.

Tabela 4 "Tarefas Desenvolvidas por Departamento" (Fonte Própria, 2018)

No decorrer das tarefas enunciadas, foi identificada a entrada em vigor do Novo Regulamento Geral de Proteção de Dados Pessoais que impôs a revisão dos processos

de tratamento dos Dados Pessoais dos clientes e dos colaboradores, e a implementação de processos de tratamento atualizados de forma a garantir a conformidade das operações hoteleiras e administrativas como Regulamento. No capítulo seguinte, são descritas as medidas organizacionais, técnicas e jurídicas propostas para responder aos requisitos impostos pelo RGPD.

4.1. A Implementação do RGPD na Hotelaria

Após a interpretação dos pressupostos e requisitos do Regulamento Geral de Proteção de Dados Pessoais foi delineado um plano de ação composto por onze categorias diferentes de medidas a implementar. As medidas - descritas nos subcapítulos seguintes - foram implementadas nos termos do cronograma seguinte. Tendo em conta a entrada em vigor do Regulamento a 25 de maio de 2018, foi proposto um cronograma – constante na Tabela 6 - que permitisse libertar os dois meses anteriores à entrada em vigor para notificações legais e eventuais melhorias às medidas a implementar.

	set 17	*out 17*	*nov 17*	*dez 17*	*jan 18*	*fev 18*	*mar 18*	*abr 18*	*mai 18*
Definição do Encarregado de Proteção dos Dados (DPO)									
Definição da equipa permanente (Comité de Proteção de Dados)									
Inventariar os processos de tratamento e Dados Pessoais recolhidos									
Definição das medidas de Proteção "*Privacy by Design/Default"*									
Revisão dos contratos com "subcontratantes" e com Terceiros									
Revisão e atualização da Política de Privacidade e o do Código de Conduta									
Atualização do processo de informação e consentimento									
Implementação do portal de acesso aos direitos dos titulares									
Elaboração das avaliações de risco (DPIA)									
Elaboração dos processos de notificação por violação de dados									
Notificação à CNPD dos tratamentos realizados									

Tabela 5 "Cronograma das atividades desenvolvidas ao longo da implementação do RGPD" (Fonte Própria, 2018)

Cada um destes grupos de medidas, foi implementado em conjunto com departamentos determinados. Na tabela seguinte, refletem-se as relações entre as medidas a implementar e os departamentos intervenientes no processo.

Medida a implementar	Departamento
Definir o Encarregado de Proteção dos Dados (DPO)	Departamento de Administração
Definir equipa permanente (Comité de Proteção de Dados)	Departamento de Administração
Inventariar os processos de tratamento, e os documentos utilizados e avaliar conformidade de tratamento à luz do RGPD	Departamento de Operações Departamento de Marketing Departamento de Recursos Humanos Departamento Jurídico Departamento Tecnologias da Informação Direções de Hotéis
Definir as medidas de Proteção *Privacy by Design/ Default*	Departamento de Administração Departamento Tecnologias da Informação
Rever os contratos com "Subcontratantes" e Terceiros	Departamento de Administração

	Departamento Jurídico
Rever e redigir Política de Privacidade e Código de Conduta	Departamento de Administração Departamento Jurídico Departamento Tecnologias da Informação Departamento de Operações Departamento de Marketing Departamento de Recursos Humanos Direções de Hotéis Receções
Implementar processo de informação e de recolha de consentimento	Departamento de Administração Departamento Tecnologias da Informação Departamento Jurídico Departamento de Marketing Departamento de Recursos Humanos Departamento de Operações Direções de Hotéis Receções
Implementar a estrutura de acesso aos Direitos dos Titulares	Departamento de Administração Departamento Tecnologias da Informação Departamento Jurídico
Elaborar uma avaliação de risco DPIA	Departamento de Administração Departamento Tecnologias da Informação Departamento Jurídico
Elaborar processo de notificação por violação de dados	Departamento de Administração Departamento Tecnologias da Informação Departamento Jurídico
Notificar a Comissão Nacional de Proteção de Dados dos tratamentos realizados	Departamento de Administração Departamento Tecnologias da Informação Departamento Jurídico

Tabela 6 Medidas e desenvolver no âmbito do RGPD por Departamento" (Fonte Própria, 2018)

4.2. Definição do Encarregado de Proteção dos Dados (DPO)

A primeira medida a implementar foi a definição do modelo relativo ao Encarregado de Proteção dos Dados. Nos termos do artigo 7.º do Regulamento o Encarregado de Proteção dos Dados (DPO) deve ser nomeado, quando a entidade que trate os dados seja: uma autoridade pública; uma organização que realize monitoramento sistemático em larga escala; ou uma organização que se envolva em processamento em grande escala de Dados Pessoais sensíveis (ensaios clínicos, dados médicos em geral). Deverá ser criada uma figura de DPO quando o tratamento dos dados, pela qualidade ou quantidade, represente elevados riscos para os titulares dos dados. Nestas situações tem de ser criado um cargo de DPO, como parte integrante da organização que desempenha as suas funções de forma independente[61].

[61] Artigo 37 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

Nos termos do RGPD, a obrigatoriedade da constituição de um DPO na empresa tem de ser verificada caso a caso. Não sendo obrigatória no caso em análise foram propostas várias soluções à administração:

- A primeira opção assente na requalificação de pessoal já integrado nos quadros da empresa exercendo outras funções e atribuições dentro da empresa - desde que estas não resultassem num conflito de interesses[62].

- A segunda opção assente na contratação de um DPO para integração nos quadros da empresa a tempo parcial, ou a tempo total em conjugação com outra função não incompatível;

- A terceira opção, proposta após a realização de várias reuniões e pedidos de orçamento a empresas de tecnologia informática e consultoria, passou pela contratação de uma empresa externa, em regime de *outsourcing*, que fornece o serviço em formato de *DPO as-a-service;*

- E por último, foi abordada a possibilidade de não constituir um DPO*.*

De entre outras funções já enunciadas no segundo capítulo, o encarregado da proteção de dados deve informar e aconselhar o responsável pelo tratamento, cooperar com a autoridade de controlo e ser o ponto de contacto sobre questões relacionadas com o tratamento, incluindo a consulta prévia. Por este motivo, o *Data Protection Officer* deve reportar ao mais alto nível dentro da empresa.

Devido às suas responsabilidades e conhecimentos adquiridos relativos às práticas do negócio da empresa, foi proposto que o DPO estivesse contratualmente vinculado a obrigações de sigilo e de confidencialidade no exercício das suas funções [63].

De forma a comunicar este novo cargo e as suas funções aos restantes colaboradores do grupo, foi desenvolvido um capítulo específico no Código de Conduta onde foram enumeradas as responsabilidades que o DPO nomeado deverá dar resposta. No constam as seguintes normas:

- O encarregado da proteção de dados é o responsável por documentar os procedimentos operacionais, atualizá-los e disponibilizá-los para todos os colaboradores interessados;

[62] Artigo 38.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[63] Artigo 37.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

- O DPO deverá organizar uma sessão anual de informações, enviar atualizações regulares sobre políticas e procedimentos relevantes para as suas funções;

- Ao DPO compete prestar aconselhamento, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a realização das avaliações de impacto sobre a proteção de dados e consulta prévia;

- O DPO controla a conformidade com a Lei em vigor e com as políticas relativas à proteção de Dados Pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados e as auditorias correspondentes;

- O DPO acompanha e colabora no desenvolvimento dos processos para responder aos pedidos de acesso dos titulares, correção e apagamento de dados a pedido do titular, retira o consentimento para determinados tratamentos, procede à portabilidade dos dados, se tecnicamente viável, limita o tratamento para fins de marketing direto e faz a revisão manual de decisões automáticas:

- O DPO coopera ainda com a autoridade de controlo nas questões relacionadas com o tratamento, incluindo a consulta prévia e define as funções e responsabilidades, bem como os procedimentos para fornecer feedback e notificar a Comissão Nacional de Proteção de Dados (CNPD) em caso de violação de Dados Pessoais.

Para além destas funções, foi ainda definido que o encarregado fornecer a formação apropriada para colaboradores com acesso legítimo a Dados Pessoais sobre as ferramentas que eles usam em conexão com seu trabalho[64].

4.3. Definição da equipa permanente (comité de proteção de dados)

Para além do *Data Protection Officer,* o Regulamento refere a necessidade de formar uma equipa multidisciplinar de forma a responder adequadamente e com caracter de permanência à complexidade do RGPD.

Para este efeito foi proposto o desenho de um Comité de Proteção de Dados formado por elementos do Departamento de Marketing, Departamento de Tecnologias de Informação, Departamento Jurídico, Departamento de Operações, Departamento de Serviços Administrativos e Financeiros, Departamento de Vendas, Departamentos de Reservas e Departamento de Qualidade que em conjunto com elementos da Administração e com DPO acompanhe a implementação e manutenção do RGPD.

[64] Artigo 37.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

O organograma abaixo, consta do Código de Conduta, das Avaliações de Risco e os demais documentos respeitantes à Proteção de Dados da Empresa.

Figura 3 "Organograma DPO e Comité de Proteção de Dados" (Fonte Própria 2018)

O DPO deverá reunir periodicamente com o Comitê de Proteção de Dados e Privacidade.

4.4. Inventário de dados, documentos e formas de tratamento

Depois de proposto o modelo do Comité de Proteção de Dados e da sua relação com o Encarregado de Proteção dos Dados, foram desenvolvidos um conjunto de inventários, que visaram responder às seguintes questões:

- Que Dados Pessoais eram recolhidos?
- Que documentos estavam a ser utilizados para recolher os Dados Pessoais?
- Quem recolhia os Dados Pessoais?
- Onde eram arquivados e armazenados os Dados Pessoais?
- Como eram recolhidos os Dados Pessoais?
- Quais os fins para os quais os Dados Pessoais eram tratados?

Na maior parte das operações hoteleiras os Dados Pessoais são tratados de forma a desenvolver a exploração de empreendimentos turísticos: garantir a celebração de contratos de hospedagem e de outros serviços conexos; gerir as disponibilidades dos quartos e das tarifas; e comunicar informações e promoções através de correio eletrónico, SMS ou chamada telefónica.

Relativamente às reservas, podemos encontrar dois momentos cronologicamente distintos em que é feita a recolha de Dados Pessoais pelo hoteleiro. Um momento inicial em que é realizada a recolha de dados para ser proceder à reserva e um momento posterior em que é efetuada a prestação de serviço propriamente dita, iniciada com o *check-in* e concluída com o check-out e a faturação.

Estes dois momentos podem ser mais ou menos distanciados no tempo ou simultâneos, como no caso das reservas ao balcão - *walk-in* - mas normalmente consubstanciam-se em operações diferentes.

Na generalidade dos hotéis, os Dados Pessoais dos hóspedes são recolhidos diretamente por funcionários quando contactados por correio eletrónico ou por telefone, ou facultados diretamente pelo cliente em formulários eletrónicos em reservas *online*. Os dados recolhidos ficam armazenados em bases de dados num sistema de *Enterprise Resource Planning* (ERP). Os Dados Pessoais são inseridos no *software* de gestão e é criada uma ficha de cliente armazenada de forma lógica na base de dados. Todos os registos efetuados ficam associados aos respetivos utilizadores.

Os *Enterprise Resource Planning* são sistemas de informação que integram todos os dados e processos da organização num único sistema e em que a informação pode ser vista sob uma perspetiva funcional - sistemas de finanças, contabilidade, recursos humanos, produção, marketing, vendas, compras, etc. - e sob uma perspetiva sistemática - sistema de processamento de transações, sistemas de informações de gestão, sistemas de apoio a decisão etc. Armazenada desta forma possibilita a automatização e visualização de todas as informações do negócio.

Para proceder à reserva o interessado faculta os seguintes seus Dados Pessoais: nome, sexo e endereço de correio eletrónico. Para além do consumidor final, também distribuidores intermediários disponibilizam Dados Pessoais dos utilizadores para efeitos de reserva ao abrigo dos acordos de confidencialidade celebrados. Após ser gravada a reserva, o sistema envia automaticamente ao titular dos dados uma mensagem de correio eletrónico contendo todas as informações legais e contratuais.

No momento do *check-in*, são recolhidos adicionalmente, morada (endereço, código postal, localidade, cidade, concelho, distrito, país), número de identificação, número de telefone de contacto e a nacionalidade. Os colaboradores no hotel verificam a veracidade e atualidade dos dados recolhidos através da análise de cartões comprovativos (cartão de identificação ou passaporte). Aquando da inserção dos Dados Pessoais na aplicação,

o *software* de gestão verifica automaticamente as informações do perfil individual e propõe o preenchimento dos dados requeridos quando os campos estejam incompletos ou não preenchidos. O cliente é responsável por fornecer os Dados Pessoais corretos para efeitos de faturação.

Para além dos pedidos de reserva, os hóspedes interessados em receber *newsletter* e outras informações comerciais consentem expressamente o seu envio. Nesse momento e para finalidades de adesão a programas de fidelização são recolhidos e tratados os nomes e endereços de correio eletrónico dos interessados, assim com o seu consentimento.

Figura 4 "Descrição funcional da realização de reservas" (Fonte Própria, 2018)

No momento do inventário, foram registados os seguintes processos de recolha de Dados Pessoais:

- Para fins contratuais e de contacto futuro: o nome, o género, o endereço de correio eletrónico e o número de telefone;

- Para fins contratuais e de controlo de qualidade de serviço: as preferências de quarto, alimentação, alojamento e dados referentes a viaturas próprias ou alugadas.

- Para fins contratuais e cumprimento de obrigações legais, nomeadamente a identificação do hóspede: o número de identificação ou, no caso de o hóspede ter nacionalidade de país não membro da União Europeia, os dados referentes ao seu passaporte para posterior comunicação ao Serviço de Estrangeiros e Fronteiras;

- Para fins contratuais e de programa das de fidelização: os números de utilizador frequente ou de membro de clube.

- Para efeitos legais de faturação são recolhidos o nome, Número de Identificação Fiscal e morada;

- Para fins contacto futuro e comunicações de produto a pedido do cliente: o nome, o endereço de correio eletrónico e o número de telefone.

4.5. Implementação de Medidas de Proteção Privacy *by* Design, Privacy *by* Default

Em função dos inventários levantados, dos dados recolhidos, finalidades e processos de tratamento, foram, em seguida, elaboradas um conjunto de medidas com vista a implementação de uma política de gestão de privacidade dos dados por desenho e por padrão .

A Política de Privacidade por *design and default* - por desenho e por padrão- refere-se a um conceito desenvolvido por Ann Cavoukian na década de 1990 no Estado do Ontário e que tem sido adotado nos últimos anos por reguladores de todo o mundo como uma componente essencial da proteção de privacidade[65]. Este conceito tem como visão que o "futuro da privacidade não pode ser assegurado apenas por conformidades com os quadros reguladores" e de que "a privacidade deve partir de um modo padrão de operação da própria organização" para garantir a segurança e obter uma vantagem competitiva sustentável sobre as outras empresas[66].

A adoção deste modelo, têm sobretudo relevância, nos produtos e nas indústrias ligadas aos equipamentos mobile - aplicações para telemóveis, *tablets* e outros serviços de internet - onde o desenvolvimento frequente e contínuo de novos produtos deve passar a respeitar em permanência as garantias exigidas pela legislação. Ao contrário, nos sectores de atividade que ofereçam produtos ou serviços mais tradicionais e com ciclos

[65] Cavoukian, A. (2009). Privacy by Design, The 7 Foundational Principles". Canada: Information and Privacy Commissioner of Ontario.

[66] Cavoukian, A. (2009). Privacy by Design, The 7 Foundational Principles". Canada: Information and Privacy Commissioner of Ontario.

de vida mais longos, como a hotelaria – em que será mais fácil garantir uma aplicação continuada destas regras ao tratamento de Dados Pessoais. Na hotelaria, os serviços são estruturados para respeitarem os requisitos do RGPD e poderão subsistir em conformidade por um período maior de tempo, independentemente de futuros desenvolvimentos e melhorias que venham a ser realizados no âmbito da segurança e proteção da privacidade.

As principais medidas propostas por Ann Cavoukian (2009) visam garantir que as empresas adotem uma abordagem proativa, que garantisse uma proteção incorporada nas tecnologias de informação sem diminuição das funcionalidades dos sistemas de informação de forma a assegurar que todas as partes interessadas operem de acordo com os objetivos declarados e sempre sujeitos a avaliações independentes [67].

Os princípios da Politica de Privacidade por *design and default* podem ser aplicados a todos os tipos de informações pessoais, mas devem ser aplicados com especial atenção aos Dados Pessoais sensíveis, como informações médicas ou dados financeiros.

Estes princípios são adotados pelo Regulamento Geral de Proteção de Dados de uma forma genérica. Nos termos do artigo 25.º do RGPD, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas a proteger os direitos dos titulares dos dados. Embora os responsáveis pelos tratamentos sejam obrigados a implementar medidas técnicas e organizacionais para proteger os dados contra o tratamento ilícito, o Regulamento não define quais os requisitos específicos a implementar neste sentido, levantando apenas hipóteses nesse sentido. Uma dessas orientações é a pseudonimização. Nos termos do artigo 4.º do RGPD, pseudonimizar significa tratar os Dados Pessoais "de forma a que deixem de poder ser atribuídos a um titular de dados especifico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os Dados Pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável". Este processo pode ser atingido quando os campos de identificação contidos num registo de dados são substituídos por um ou mais identificadores artificiais não permitindo a identificação do titular dos dados.

[67] Cavoukian, A. (2009). Privacy by Design, The 7 Foundational Principles". Canada: Information and Privacy Commissioner of Ontario.

Outro requisito programático do regulamento define que responsável deve aplicar as medidas técnicas e organizativas que permitam assegurar que, por defeito, só sejam tratados os Dados Pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de Dados Pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, estas medidas acautelar, que por defeito, os Dados Pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Em função do inventário realizado no ponto anterior foram delineadas um conjunto de medidas técnicas e organizacionais que oferecem resposta, nos termos do artigo 25.º do RGPD, aos pressupostos deste princípio.

As medidas propostas para implementação foram:

- A minimização os dados recolhidos e tratados: a avaliação e eliminação de dados e campos de recolha desnecessários (por exemplo, número de filhos, nome de solteira, números de contacto de emergência, hobbies, habilitações, etc.);

- A opção pela pseudonimização dos nomes dos titulares de dados quando não existem dados que permitam ações de marketing ou comunicação (e-mail, telefone);

- A opção pela cifragem[68] de dados a conservar por períodos mais longos para fins estatísticos;

- A estipulação dos prazos de eliminação de Dados Pessoais para quando os mesmos atinjam o prazo estipulado e a implementação de ferramentas informáticos que eliminem os dados quando estes deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento, ou quando o titular retire o consentimento[69];

- A verificação das garantias de confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento e a implementação de um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento[70];

- A verificação da necessidade de procedimentos de certificação em matéria de proteção de dados, como selos e marcas de proteção de dados, para efeitos de comprovação da

[68] A cifragem significa que os dados são codificados de forma a que apenas podem ser lidos por pessoas autorizadas.
[69] Nos termos do artigo 89.º n. º1.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[70] Nos termos do artigo 24.º e 32.º do Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o regulamento [71];

- A verificação do sistema de autenticação e do registo das atividades de tratamentos relativos aos seguintes dados[72]:

- O nome e contactos do responsável pelo tratamento;

- As finalidades do tratamento dos dados;

- A descrição das categorias de titulares de dados e das categorias de Dados Pessoais;

- As categorias de destinatários a quem os Dados Pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais:

- As transferências de Dados Pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e a documentação que comprove a existência das garantias adequadas;

- Os prazos previstos para o apagamento das diferentes categorias de dados;

- E o desenvolvimento de uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1 do RGPD.

As medidas propostas de alteração foram enviadas ao departamento de administração e de tecnologias de informação, para validação e posterior implementação.

4.6. Revisão dos contratos com "Subcontratantes" e Terceiros

O regulamento define ainda quais são os direitos e as obrigações para os responsáveis pelo tratamento dos dados, e para as empresas subcontratadas por estes - os subcontratantes[73].

Nos termos do artigo 18.º do GDPR "quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas

[71] Nos termos do artigo 42.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[72] Nos termos do artigo 30.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016
[73] Numa tradução manifestamente infeliz, define-se no artigo 4.º 8) do RGPD, "subcontratante" como, "uma pessoa singular coletiva que trate os Dados Pessoais por conta do responsável pelo tratamento destes", o que no direito português se designa comumente como subcontratado. Enquanto a definição não for alvo de substituição, continuaremos a designar o subcontratado por subcontratante.

adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados".

Após a análise das regras previstas no artigo 28.º do Regulamento foram revistos os contratos com os vários subcontratantes e feitos pedidos de esclarecimentos quanto aos termos de prestação dos vários serviços de forma a:

- Formalizar as regras relativas à confidencialidade dos Dados Pessoais confiados a terceiros. Deverá existir, nomeadamente, uma cláusula de forma a garantir a confidencialidade não apenas dos próprios funcionários do *subcontrante*, como de todos os freelancers contratados para auxiliar no desempenho de suas obrigações;

- Garantir que o terceiro não poder copiar quaisquer documentos ou meios de informação que lhe sejam confiados, com exceção dos necessários para realizar o serviço planeado;

- Garantir que o terceiro deve obter o acordo prévio do hotel para todas as operações: não deve usar os documentos e informações processadas para fins diferentes dos especificados; não deve divulgar os documentos ou informações a outras pessoas, públicas ou privadas, naturais ou legais; deve tomar todas as medidas necessárias para evitar qualquer uso impróprio ou fraudulento dos arquivos de computador;

- Garantir que o terceiro está obrigado a tomar todas as medidas de segurança (especificamente no que diz respeito ao *hardware*) para garantir a preservação e integridade dos documentos e informações processadas ao longo da duração do relacionamento e, quando a relação termina, destruir todos os arquivos apresentar a política de segurança física e lógica implantada pelo subcontratante, além das medidas aplicáveis em caso de intrusão dolosa[74];

- Garantir que o terceiro está obrigado a implementar medidas para garantir a eficácia das garantias de proteção de dados do subcontratado, realizando auditorias de segurança, certificação da gestão de segurança dos Dados Pessoais. O contrato celebrado deve conter as disposições presentes no n. ° 3 do artigo 28. ° do RGPD, nomeadamente, o objeto e a duração do tratamento de Dados Pessoais, a finalidade do tratamento e as obrigações de segurança;

- Garantir que o terceiro está obrigado a desenvolver as ferramentas e recursos operacionais e contratuais necessários para rescindir o relacionamento com o prestador de serviços, mais especificamente em caso de violação de contrato e esclarecimentos adicionais caso esses dados sejam mantidos em formato *cloud*;

[74] Torres, C. (2016). Les BCR sous-traitants, un instrument d'encadrement des flux. Disponível em alain-bensoussan.com

- Garantir que o terceiro está obrigado a formalizar as condições para devolver os dados e destruí-los em caso de violação do contrato ou no final do contrato[75];

- Garantir a existência de cláusulas contratuais-tipo se os dados forem transferidos para fora da União Europeia para um país considerado não adequado. No caso de os dados serem transferidos para os Estados Unidos, existe um regime específico de privacidade, nomeado de *Privacy Shield*, do qual daremos nota mais adiante;

- Garantir que o subcontratante está impedido de contratar outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral.

As conclusões foram enviadas ao departamento de administração e jurídico, para validação e posterior implementação.

4.7. Revisão e redação de alterações à Política de Privacidade e Código de Conduta

Após a revisão dos contratos com os terceiros foi elaborada uma proposta de atualização da Política Privacidade e de Proteção de Dados. O objetivo das alterações sugeridas foi aumentar e consolidar a informação da política de privacidade anterior e partilhá-la com colaboradores e clientes.

Anterior	Alteração Sugerida
O Grupo (...) tem como compromisso assegurar um serviço de qualidade a todos os clientes e visitantes do site, bem como aspetos que se relacionem com a sua privacidade.	O Grupo (...) tem como compromisso assegurar um serviço de qualidade a todos os clientes e visitantes do site, assim como a todos os aspetos que se relacionem com a sua privacidade. Todas as informações pessoais relativas a membros, clientes ou visitantes são tratadas de acordo com a Lei da Proteção de Dados Pessoais. O Grupo (...) preza a sua privacidade e por isso, quer seja um utilizador recente ou de longa data, pedimos que leia a nossa politica de privacidade e se tiver dúvidas, não hesite em contactar-nos. O uso do nosso site pressupõe a aceitação desta Política de Privacidade.

[75] Avignon, C. (2016). La décision d'adéquation pour l'EU-US Privacy Shield. Disponível em alain-bensoussan.com

PROTECÇÃO DA INFORMAÇÃO INFORMAÇÃO PESSOAL	PROTECÇÃO DA INFORMAÇÃO INFORMAÇÃO PESSOAL
Os seus contatos são utilizados na nossa base de dados igualmente para envio de informações relativas a promoções, vigentes na nossa Newsletter semanal. Dados de informação pessoal são-lhe pedidos de forma a poder aceder ao programa de fidelização, bem como no ato de marcação de reserva em qualquer unidade. De notar que toda a sua informação pessoal será usada somente para efetivação da respetiva reserva.	O Grupo (...) recolhe informações para prestar melhores serviços a todos os seus clientes. Quando partilha informações connosco, por exemplo, ao fazer uma reserva ou ao criar uma conta no nosso site dá-nos a possibilidade de melhorar ainda mais esses serviços. Desde perceber o idioma que fala e como poderemos personalizar a sua reserva ao envio de informações relativas a promoções vigentes na nossa Newsletter semanal. Por exemplo, antes de fazermos uma reserva recolhemos os Dados Pessoais necessários para a efetivar, ou aquando da inscrição no programa de fidelização, solicitamos informações pessoais, como o nome, o endereço de E-mail, para armazenar com a sua conta, para que possa tirar o máximo partido das funcionalidades que disponibilizamos. Os dados são recolhidos de uma forma correta e lícita, sem exceder o intuito original para o qual foram recolhidos.
Os seus dados não serão transmitidos a entidades terceiras, mas somente para uso exclusivamente interno ao Grupo (...).	Os seus dados não são transmitidos a entidades terceiras sem o seu consentimento, quando este for exigido por lei, exceto nos casos previstos neste documento, e são conservados até 2 anos a contar da ultima interação com os nossos serviços ou hotéis, ou, enquanto o cliente beneficiar do programa de fidelização, se em data posterior.
Se já é um cliente registado no nosso site, poderá alterar os seus Dados Pessoais sempre que pretender, bastando inserir o seu Utilizador e palavra-passe.	Se já é um cliente registado no nosso site, poderá alterar os seus Dados Pessoais sempre que pretender, bastando inserir o seu Utilizador (Username) e palavra-passe (password).
COOKIES	COOKIES
Quando visitar o nosso site, um pequeno ficheiro de texto (Cookie) é criado e gravado no disco do seu computador. Este ficheiro ao reconhecê-lo, vai permitir-lhe uma maior facilidade e rapidez no acesso, e personalização da página a nível da sua experiência online. Identificamos também informação técnica do seu computador quando visita as páginas do nosso site, como o IP (Internet Protocol), o sistema operativo, o tipo de browser. Utilizamos esta	Quando visitar o nosso site, um pequeno ficheiro de texto (Cookie) é criado e gravado no disco do seu computador. Este ficheiro ao reconhecê-lo, vai permitir-lhe uma maior facilidade e rapidez no acesso, e personalização da página a nível da sua experiência online. Identificamos também informação técnica do seu computador quando visita as páginas do nosso site, como o IP (Internet Protocol), o sistema operativo, o tipo de browser. Utilizamos esta informação para

informação para melhorar a qualidade da sua visita ao nosso site, e não a divulgaremos a entidades externas ao Grupo.	melhorar a qualidade da sua visita ao nosso site, e não a divulgaremos a entidades externas ao Grupo.
A maioria dos browsers aceita automaticamente estes ficheiros (Cookies), mas poderá apagá-los ou definir automaticamente o seu bloqueio.	A maioria dos browsers aceita automaticamente estes ficheiros (Cookies), mas poderá apagá-los ou definir automaticamente o seu bloqueio.
No menu "Help" do seu browser encontrará como efectuar essas configurações. No entanto, caso não permita o uso de cookies poderá haver algumas funcionalidades que não conseguirá utilizar.	O utilizador pode ainda configurar o seu navegador para bloquear todos os cookies, incluindo cookies associados aos nossos serviços, ou para indicar quando um cookie está a ser instalado por nós. No entanto, é importante não esquecer que alguns dos nossos serviços poderão não funcionar corretamente se os cookies estiverem desativados. Por exemplo, poderemos não conseguir memorizar as preferências de idioma.
E-MAIL Se subscrever no nosso site a Newsletter, receberá por e-mail informação sobre as nossas promoções e destaques. Caso pretenda não receber mais Newsletters, poderá remover o seu endereço da nossa mailing list, clicando no link apresentado no rodapé de cada newsletter. Se é um cliente registado poderá modificar os seus Dados Pessoais a qualquer altura, bastando inserir o seu User Id e Password.	E-MAIL Se subscrever no nosso site a Newsletter, receberá por e-mail informação sobre as nossas promoções e destaques. Caso pretenda não receber mais Newsletters, poderá remover o seu endereço da nossa mailing list, clicando no link apresentado no rodapé de cada newsletter. Se é um cliente registado poderá modificar os seus Dados Pessoais a qualquer altura, bastando inserir o seu User Id e Password.
SEGURANÇA	SEGURANÇA Trabalhamos arduamente no sentido de proteger os nossos utilizadores de acesso não autorizado a ou alteração, divulgação ou destruição não autorizadas de informações que se encontram na nossa posse.
Para garantir a segurança dos seus dados e a máxima confidencialidade, tratamos a informação que nos forneceu de forma absolutamente confidencial, de acordo com as nossas políticas e procedimentos internos de segurança e confidencialidade.	Para garantir a segurança dos seus dados e a máxima confidencialidade, tratamos a informação que nos forneceu de forma absolutamente confidencial, de acordo com as nossas políticas e procedimentos internos de segurança e confidencialidade. No caso de o cliente contratar serviços dos nossos hotéis no Brasil, poderá transferir os dados dentro do âmbito da sua organização de forma a melhor adequar a oferta e a conveniência dos nossos serviços. O Grupo (...) tomou as garantias adequadas à sua transmissão pelo procedimento

	em clausulas-tipo de proteção de dados adotado pela Comissão Europeia.
Sempre que lhe for solicitada informação do cartão de crédito, esta comunicação é efectuada através de linha segura SSL (Secured Sockets Layer), quando estiver a utilizar browsers que permitam SSL, tais como Microsoft Internet Explorer ou Netscape Navigator. Utilizaremos também SSL em todas as páginas onde lhe for solicitada informação pessoal, o que significa que a sua informação será enviada através da Internet de forma encriptada. Poderá verificar que está em modo seguro quando visualizar um icon cadeado ou chave no canto inferior direito ou no canto inferior esquerdo do seu ecrã.	Sempre que lhe for solicitada informação do cartão de crédito, esta comunicação é efectuada através de linha segura SSL (Secured Sockets Layer), quando estiver a utilizar browsers que permitam SSL, tais como Microsoft Internet Explorer ou Netscape Navigator. Utilizaremos também SSL em todas as páginas onde lhe for solicitada informação pessoal, o que significa que a sua informação será enviada através da Internet de forma encriptada. Poderá verificar que está em modo seguro quando visualizar um *icon* cadeado ou chave no canto inferior direito ou no canto inferior esquerdo do seu ecrã. Direito de acesso aos dados Os nossos clientes têm diferentes preocupações de privacidade e podem a qualquer momento rever, atualizar e decidir que tipo de dados, pretendem ver guardados. No nosso Portal podem consultar e controlar determinados tipos de informações associadas à sua conta, obter informações, visualizar e editar as suas preferências, pedir o apagamento ou a portabilidade dos seus Dados Pessoais, bastando para isso inserir o seu User Id e Password. O responsável pelos dados pode ser contactado diretamente através do e-mail. DIREITOS DE PROPRIEDADE INTELECTUAL Todos conteúdos presentes neste site são propriedade do Grupo (...) (textos, imagens) e estão protegidos pelo Código do Direito de Autor e dos Direitos Conexos. Este site pode conter links para sites de terceiros que não estão sob o controle do Grupo (...).

Tabela 7 Proposta de alteração de Politica de Privacidade (Fonte Própria, 2018)

As propostas de alteração foram enviadas ao departamento jurídico e de tecnologias de informação, para validação e posterior publicação.

Foi ainda atualizado o Manual de Conduta de forma a refletir os considerandos do regulamento relativamente aos comportamentos a observar pelos colaboradores nas suas relações com os Dados Pessoais dos clientes e com os sistemas de informação.

Os objetivos que se pretenderam atingir com este manual foram: evidenciar a conformidade do Grupo e dos seus processos com o RGPD; detalhar as funções dos órgãos, evidenciando a repartição destas funções pelo pessoal administrativo e operacional; definir os processos de trabalho e da gestão da privacidade e proteção dos dados; e tornar a informação facilmente acessível a todo o pessoal envolvido.

A utilização das ferramentas informáticas e dos Dados Pessoais são essenciais ao bom funcionamento da empresa e a utilização deve ser rigorosa de modo a não comprometer o desempenho dos demais colaboradores da empresa e da imagem do hotel. O manual de conduta é, por si só, um instrumento para demonstração de conformidade e as normas nele constantes têm de ser comunicadas a todos os colaboradores de forma a serem cumpridas.[76].

As propostas de alteração foram enviadas ao departamento jurídico e de tecnologias de informação, para validação e posterior publicação.

Paralelamente ao manual de normas foi também proposta ao Departamento Jurídico a adição de uma cláusula de confidencialidade relativa à proteção de dados, para os contratos de trabalho futuros e para os contratos já existentes.

4.8. Implementação dos processos de informação e pedido de consentimento aos titulares dos dados.

O regulamento define as circunstâncias em que os Dados Pessoais e os consentimentos dos titulares são recolhidos. Existem para esse efeito um conjunto de exigências para obtenção dos consentimentos, sendo que, em caso de não cumprimento, o responsável pelo tratamento, fica obrigado à obtenção de um novo consentimento.

Em primeiro lugar, e nos termos do artigo 13.º e seguintes do Regulamento, no momento da recolha dos Dados Pessoais o responsável pelo tratamento é obrigado a disponibilizar um conjunto de informações ao cliente. Este texto informativo tem de conter todas as disposições legais, nomeadamente, a identidade e os contactos do responsável pelo tratamento, os contactos do encarregado da proteção de dados, as finalidades do tratamento a que os Dados Pessoais se destinam, o fundamento jurídico do tratamento, os destinatários ou categorias de destinatários dos Dados Pessoais e os processos para

[76] Artigo 5º, 24º e 39º do Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

serem efetuados os pedidos de acesso, retirada do consentimento, retificação, apagamento, limitação, portabilidade e a oposição ao tratamento e todas as demais informações legais necessárias à informação. Esta informação contem ainda todas as informações relativas à Política de Privacidade e de Proteção, e nele deve também constar o pedido para o consentimento explícito do interessado a solicitar o envio de informações de marketing por correio eletrónico e SMS, caso o se pretenda.

Para dar resposta a estes requisitos, foram desenvolvidas propostas de textos informativos com vista à informação e à obtenção de consentimento dos particulares em língua em portuguesa e inglesa e pedidas subsequentes traduções para outras línguas a tradutores especialistas.

De forma a criar uma mensagem concisa, transparente e inteligível foi proposto um modelo de comunicação com uma formulação tipicamente anglo-saxónica *(what, who, when, why, how)*, mais eficaz para este tipo de comunicações do que o modelo contratual ou de articulado.

Foi proposta aos departamentos de administração e jurídico a seguinte versão em português:

"Como e para que fins os seus Dados Pessoais são utilizados?
O Grupo X.X. utiliza a informação recolhida para facilitar os processos de reserva de quartos e faturação, gestão de clientes, para fins históricos e estatísticos, obrigações legais, controle da qualidade de serviço e para contactos futuros. Utilizamos a informação recolhida para adequar os nossos produtos e serviços aos nossos clientes, para o envio de informações, promoções e prémios em função das estadias, através de correio eletrónico, SMS ou chamada telefónica. Esta comunicação é relativa aos nossos produtos ou produtos de parceiros com os quais tenhamos acordo e não constitui uma obrigação legal ou contratual.
Não existem consequências para quem não as fornecer.

Quem é o responsável pela informação?
O Grupo X.X. é o responsável pelos dados recolhidos que são tratados informaticamente. A informação é utilizada no âmbito do seu grupo empresarial composto pelas seguintes sociedades: (...). Para garantir a segurança dos seus dados e a máxima confidencialidade, tratamos a informação que nos forneceu de forma absolutamente confidencial, de acordo com as nossas políticas e procedimentos internos de segurança e confidencialidade e não partilhamos os seus dados com terceiros para fins comerciais. Podem existir decisões automatizadas, como a definição de perfis, de forma a melhor adequar a nossa oferta às necessidades dos nossos clientes e a permitir que clientes aderentes ao (...) recebam promoções e benefícios específicos. O Grupo X.X. pode recorrer a terceiros para o envio de e-mails e SMS.

O titular dos dados pode apresentar reclamação à autoridade de controlo – a Comissão Nacional de Proteção de Dados.

Quem posso contactar para aceder, retificar ou apagar os dados?
Os nossos clientes e visitantes têm diferentes preocupações de privacidade e podem a qualquer momento rever, atualizar e decidir que tipo de dados pretendem ver guardados. O encarregado pelos dados pode ser contactado diretamente através do e-mail ou por correio (...) a quem poderá solicitar a qualquer momento a cópia dos dados que lhe digam respeito, a retirada do consentimento, a retificação, o apagamento, a limitação, a portabilidade e a oposição ao tratamento dos mesmos. No nosso site podem consultar e controlar determinados tipos de informações associadas à sua conta, obter informações, visualizar e editar as suas preferências, pedir o apagamento ou a portabilidade dos seus Dados Pessoais, bastando para isso inserir o seu Use Id e Password. A retirada posterior de consentimento não compromete a legalidade do tratamento realizado com base neste consentimento.

Por quanto tempo são os dados armazenados?
Os Dados Pessoais são mantidos até se esgotar o fim a que se destinam, sendo eliminados 2 anos a contar da última interação do cliente com os nossos serviços ou hotéis, ou, enquanto o cliente beneficiar do programa de fidelização (...), se em data posterior, e se aplicável. Poderão existir disposições legais que obriguem a manter os Dados Pessoais por um período de tempo mínimo superior. "

☑ Li e aceito os termos.
☑ Autorizo o envio de informação e promoções acerca do Grupo por E-mail ou correio.
☑ Autorizo o envio de informação e promoções acerca do Grupo por SMS ou através de chamada telefónica."

Posteriormente, foi traduzido o texto para inglês, francês, alemão e espanhol.

4.9. Implementação do portal de acesso na área de cliente

O regulamento obriga ainda os responsáveis pelo tratamento de Dados Pessoais, a garantir o exercício de um conjunto de direitos aos titulares dos dados. Os titulares dos Dados Pessoais têm o direito a solicitar a qualquer momento o acesso e a cópia dos seus Dados Pessoais, a retirada do consentimento que tenham dado previamente, a retificação dos seus dados, o seu apagamento, a limitação do tratamento, a portabilidade e a oposição a decisões automatizadas. Estes direitos devem ser monitorizados, documentados e passam a ter prazos máximos de resposta.

Para dar resposta aos pedidos dos clientes foi desenhado um Portal de Clientes (*One Stop-Shop*) no qual os titulares podem exercer todos os seus direitos e concebidas minutas de resposta para cada um dos processos desenhados. As seguintes propostas foram enviadas ao departamento de administração e de tecnologias de informação, para validação e posterior implementação. Em termos gerais, ao interagir com o portal, o cliente faz diretamente o pedido relativamente aos dados que lhe digam respeito e

recebe, sempre que possível, a informação por meios eletrónicos, salvo pedido em contrário do titular [77].

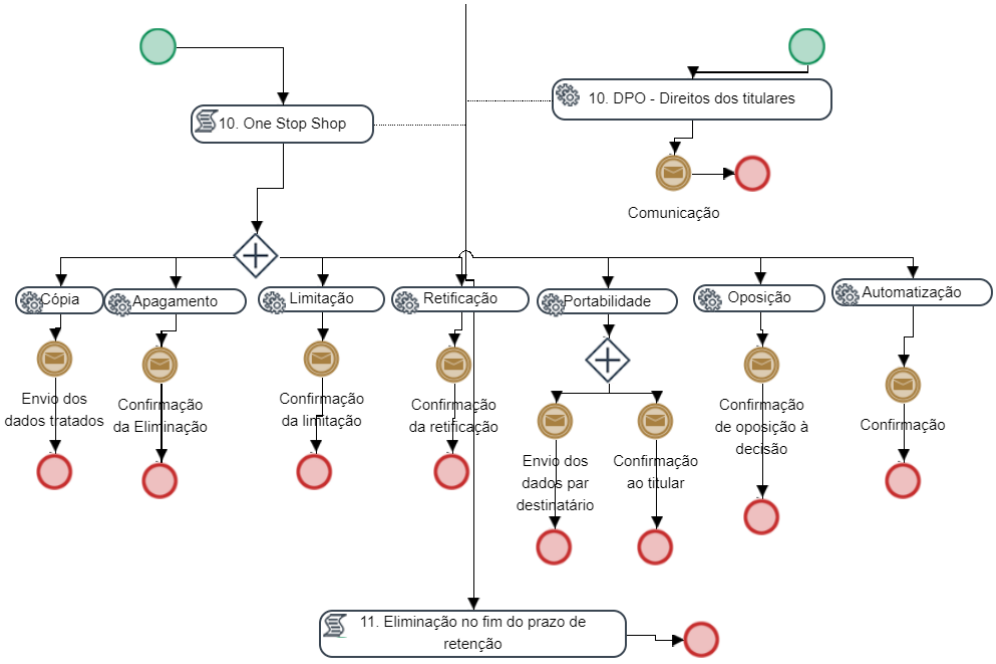

Figura 5 Processo de pedido para exercícios dos direitos dos titulares dos dados (Fonte Própria, 2018)

Nos termos do artigo 16.º do RGPD, o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os Dados Pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus Dados Pessoais e às seguintes informações:

a) as finalidades do tratamento dos dados;

b) as categorias dos Dados Pessoais em questão;

c) os destinatários ou categorias de destinatários a quem os Dados Pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

d) se for possível, o prazo previsto de conservação dos Dados Pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

[77] Nos termos do Artigo 13º-3 do Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

e) a existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos Dados Pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;

f) a direito de apresentar reclamação a uma autoridade de controlo;

g) se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

h) a existência de decisões automatizadas, incluindo a definição de perfis.

Após o login, com nome de utilizador e palavra passe pessoais, o cliente realiza o pedido na área de cliente e recebe em seguida os dados tratados num formato estruturado, de uso corrente e de leitura automática. O ficheiro com os dados tratados tem de ser entregue ao seu titular no prazo máximo de um mês.

Para o momento da resposta foi proposto o envio do seguinte texto:

Resposta e confirmação de não tratamento	Exmo. Sr. º(ª)_____ Em resposta ao pedido de acesso aos Dados Pessoais por si fornecidos aos nossos hotéis, vimos por este meio confirmar que os mesmos não são objeto de tratamento.
Envio de dados e confirmação de tratamento	Exmo. Sr. º(ª)_____ Em resposta ao pedido de acesso aos Dados Pessoais por si fornecidos aos nossos hotéis, vimos por este meio confirmar que os mesmos são objeto de tratamento pelo nosso serviço de marketing e comunicação e destinam-se ao envio de informações e promoções por E-mail, correio, SMS ou fax e a decisões automatizadas, como a definição de perfis, de forma a melhor adequar a nossa oferta às suas necessidades e áreas de interesse. Os Dados Pessoais por nós tratados são o nome, o país de origem, o endereço de e-mail, o contacto telefónico e a morada. Os dados encontram-se armazenados _____. Os seus dados serão conservados até 2 anos a contar da ultima com os nossos serviços ou hotéis, ou, enquanto beneficiar do programa de fidelização, se em data posterior, e se aplicável. Pode a qualquer momento solicitar a retificação, o apagamento, a limitação, a oposição ao tratamento

	ou apresentar reclamação à autoridade de controlo, que em Portugal é a Comissão Nacional de Proteção de Dados. Em anexo, encontra o ficheiro com os dados por nós tratados.

Tabela 8 "Minuta de resposta automática para pedidos relativos ao direito de acesso e cópia" (Fonte Própria, 2018)

Nos termos do artigo 16º do RGPD, o titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos Dados Pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus Dados Pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional[78].
Após o login, o cliente realiza o pedido na área de cliente e recebe a seguinte resposta:

Confirmação de retificação	Exmo. Sr. º(ª)_____ Em resposta ao pedido de retificação dos Dados Pessoais por si fornecidos aos nossos hotéis, vimos por este meio confirmar que os mesmos foram corrigidos e atualizados.

Tabela 9 "Minuta de resposta automática para pedidos relativos ao direito de retificação" (Fonte Própria, 2018)

O direito ao apagamento dos dados consubstancia um verdadeiro direito a ser esquecido. Nos termos do artigo 17º do RGPD, o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus Dados Pessoais, sem demora injustificada, exceto se a manutenção for necessária para cumprir uma obrigação legal (como acontece com as obrigações decorrentes do tratamento ao abrigo do regime do IVA ou do IRC) ou se ainda necessárias para cumprir as finalidades para as quais foram recolhidas (manutenção de uma reserva). Após o login, o cliente realiza o pedido na área de cliente e recebe a seguinte resposta:

Confirmação da eliminação dos dados	Em resposta ao pedido de apagamento dos Dados Pessoais por si fornecidos aos nossos hotéis, vimos por este meio confirmar que os mesmos foram eliminados pelos nossos serviços.

[78] Artigo 19.º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

Tabela 10 “Minuta de resposta automática para pedidos relativos ao direito ao apagamento” (Fonte Própria, 2018)

Nos termos do artigo 18.º RGPD, o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações: para contestar a exatidão dos Dados Pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; quando o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos Dados Pessoais e solicitar, em contrapartida, a limitação da sua utilização; quando o responsável pelo tratamento já não precisar dos Dados Pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; se o titular dos dados se tiver oposto ao tratamento até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados. Após a autenticação, com nome de utilizador e *password* pessoais, o cliente procede ao pedido na área de cliente e recebe a seguinte resposta:

Confirmação da limitação do tratamento de dados	Em resposta ao pedido de limitação dos Dados Pessoais por si fornecidos aos nossos hotéis, vimos por este meio confirmar que os mesmos foram eliminados uma vez que não procedemos ao tratamento de dados parciais.

Tabela 11 “Minuta de resposta automática para pedidos relativos ao direito à limitação” (Fonte Própria, 2018)

Nos termos do artigo 20.º do RGPD, o titular dos dados tem o direito de receber os Dados Pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável o possa impedir. O direito à portabilidade na hotelaria, pode ser exercido através do mesmo processo que os restantes, recebendo as partes envolvidas a seguinte comunicação.

Confirmação da portabilidade do tratamento de dados	Em resposta ao pedido de portabilidade dos Dados Pessoais por si fornecidos aos nossos hotéis, vimos por este meio confirmar que os mesmos foram enviados por mensagem eletrónica para o e-mail _____.

Envio do ficheiro de dados para destinatário da portabilidade	Cumprindo os termos do Artigo 20.º do Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de Dados Pessoais e à livre circulação, vimos por este meio responder ao pedido realizado pelo seu Exmo. Sr. º(ª)_____ enviando-lhe o ficheiro com os seus Dados Pessoais.

Tabela 12 "Minuta de resposta automática para pedidos relativos ao direito à portabilidade" (Fonte Própria, 2018)

4.10. Elaboração da Avaliação de Impacto da Privacidade de Dados (DPIA)

A Avaliação de Impacto da Privacidade de Dados (ou *Data Protection Impact Assessment* - DPIA) é um documento concebido para descrever o processo de tratamento de Dados Pessoais, averiguar a necessidade e proporcionalidade do tratamento e para ajudar a gerir os riscos dai resultantes para os direitos e liberdades dos titulares dos dados [79]. A Avaliação de Impacto da Privacidade de Dados avalia o risco, o impacto das ameaças na privacidade de dados e a probabilidade de ocorrência, com o objetivo de definir estratégias para a atenuar esses riscos para níveis aceitáveis através de um racional de custo-benefício.

O regulamento estabelece as condições em que existe obrigatoriedade de uma avaliação de impacto antes de serem iniciadas as operações de tratamento de dados que utilizam novas tecnologias e impliquem elevado risco para os direitos e liberdades dos titulares [80]. Neste sentido dispõe o Artigo 35 n.º1 do RGPD, "quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de Dados Pessoais".

Segundo o n.º2 do mesmo artigo, a realização de uma avaliação de impacto sobre a proteção de dados é obrigatória nomeadamente em caso de: avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no

[79] Nos termos do Artigo 35º Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

[80] Nos termos do Artigo 28º e 29º do Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; operações de tratamento em grande escala de categorias especiais de dados; ou de controlo sistemático de zonas acessíveis ao público em grande escala. Contudo, se de um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação[81].

No âmbito da implementação do RGPD, foram realizadas diversas Avaliações de Impacto da Privacidade de Dados nomeadamente ao processo de reservas, ao processo de recrutamento e de recursos humanos e a outros serviços conexos. Os resultados desta avaliação são tidos em conta na determinação das medidas tomadas para comprovar que o tratamento de Dados Pessoais está em conformidade com o RGPD.

Nos termos do artigo 36 do RGPD, sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar previamente a autoridade de controlo antes de se proceder ao tratamento de Dados Pessoais. O DPIA é um documento de grande importância para o modelo de autorregulação imposto pelo RGPD.

O modelo do processo de avaliação proposto para dar resposta ao Regulamento, foi desenhado pela Comissão de Proteção de Dados Francesa (CNIL) e concatenou os seguintes tópicos:

- Descrição sistemática das operações de tratamento previstas, a finalidade do tratamento e os interesses legítimos do responsável pelo tratamento;

- A natureza, âmbito, contexto e finalidades do processamento;

- Quais as responsabilidades dos intervenientes no tratamento?

- Quais as normas de conduta aplicáveis ao processamento?

- Que Dados Pessoais são tratados?

- Quais os destinatários?

- Descrição funcional das operações de tratamento;

[81] Nos termos do Artigo 35º n.º1 Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016

- Qual o esquema do tratamento?

- Quais os recursos dos quais os Dados Pessoais dependem (*hardware, software*, redes, pessoas, papel ou canais de transmissão de papel)?

- Avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

- De que forma as finalidades de tratamento se demonstram lícitas, especificadas, explícitas e legítimas?

- Qual a base legal que justifica a licitude do tratamento?

- De que forma a proporcionalidade e necessidade do processamento é adequada, relevante e limitada, em função das finalidades de tratamento?

- Que medidas contribuem para que os dados se mantenham atualizados?

- Qual o período de retenção dos dados?

- Medidas previstas que contribuem para os direitos dos titulares dos dados relativamente às informações fornecidas

- De que forma são os titulares dos dados informados acerca do tratamento?

- No caso das comunicações de marketing e da adesão à *newsletter*, como é recolhido o consentimento do titular dos dados?

- Como é que o titular dos dados exerce o seu Direito de portabilidade dos dados?

- Como é que o titular dos dados exerce o Direito ao apagamento (esquecimento) e retificação?

- Como é que o titular dos dados exerce o Direito à limitação do tratamento e oposição a decisões individuais automatizadas?

- Nas relações com entidades terceiras, de que forma estão identificadas as obrigações dos terceiros de forma a reduzir o risco de acesso legítimo a Dados Pessoais?

- Medidas previstas que contribuem para os direitos dos titulares dos dados relativamente à salvaguarda das transferências internacionais;

- Avaliação dos riscos para os direitos e liberdades dos titulares dos direitos;

- Medidas existentes e planeadas;

- A origem, natureza, particularidade e gravidade dos riscos são apreciados ou, mais especificamente, para cada risco (acesso ilegítimo, modificação indesejada e desaparecimento de dados) na perspetiva das pessoas em causa;

- Relativamente ao acesso indesejado de Dados Pessoais;

- Relativamente a modificações indesejadas de Dados Pessoais;

- Relativamente ao desaparecimento de Dados Pessoais;

- As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos Dados Pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

Relativamente aos principais impactos, foram considerados da perspetiva dos titulares dos dados:

- A possibilidade de ocorrência de *spam*;

- O cancelamento de reservas;

- A existência de contas *online* bloqueadas;

- A receção de publicidade não desejada;

- A negação de acesso a serviços comerciais;

- Redundâncias e percas de tempo repetindo formalidades ou aguardando que as mesmas sejam preenchidas;

- A perca de dados atualizados;

- A criação de perfis incorretos.

Por outro lado, as principais ameaças que podem conduzir a que estes riscos ocorram são tipicamente: o uso de unidades *flash* USB ou discos que não sejam adequados à sensibilidade da informação; o uso ou transporte de *hardware* sensível para fins pessoais; a observação do ecrã de uma pessoa sem o seu conhecimento, no posto de trabalho ou fora do posto de trabalho (transportes públicos); a remoção de componentes de hardware; o roubo de *laptop*; o roubo de um telefone de trabalho; a perda de um dispositivo de armazenamento eletrônico; o envio de *spam* por meio de um programa de correio eletrónico; o mau uso das funções de rede; a infeção por código malicioso; instalação de uma ferramenta de administração remota; a divulgação involuntária de informações durante uma conversa de correio eletrónico; o *phishing*; ou o roubo de arquivos de escritórios.

No decorrer da implementação do RGPD foram definidas como as principais fontes de risco para verificação destas ameaças:

- A possibilidade de *hackers* atacarem os sistemas e causam compromisso de Dados Pessoais, intercetando ou acedendo aos mecanismos de comunicação estabelecidos roubando informação, comprometendo Dados Pessoais;
- A rotação de colaboradores que desconhecem as políticas do grupo podendo causar danos operacionais ou financeiros por intencionalidade ou por más práticas;
- A exposição dos equipamentos informáticos a condições adversas que possam implicar a interrupção ou quebra do serviço;
- A disrupção nas comunicações de dados que implique a paragem do sistema informático de gestão;
- A disrupção no fornecimento de energia elétrica que implique a quebra de funcionamento do equipamento informático;
- O roubo ou o extravio de equipamento informático ou suportes de dados (disco externo, *pen*, DVD, etc.) contendo informação sensível;
- A instalação de *software* não autorizado ou de proveniência incerta podendo comprometer a segurança ou dos sistemas de informação;
- O acesso não autorizado aos servidores e postos de trabalho;
- A perda de dados;
- Os erros e as vulnerabilidades no *software.*

Para controlar as fontes de risco identificadas foram sugeridas a implementação e a manutenção de um conjunto de medidas. Entre outras:

- A implementação de programas de formação contínua de colaboradores;

- A definição de normas e de políticas de segurança informática a seguir pelos colaboradores;

- A implementação de programa de auditoria interna;

- A sujeição dos colaboradores com acesso aos Dados dos Clientes a obrigações contratuais de confidencialidade;

- A manutenção de uma metodologia e processo de acesso que exige autenticação e o acesso à rede restrito;

- Encriptação incluída na *VPN* (*Virtual Private Network* ou Rede Privada Virtual);

- A manutenção de antivírus gerido de forma centralizada, aplicado em todos os pontos terminais, como política corporativa;

- A proteção de *malware* conhecido (em base de dados) e desconhecido (por teste de comportamento);

- Procedimentos aplicados de forma centralizada para *backlisting* de *websites* maliciosos conhecidos; procurar conteúdo malicioso em todos os dispositivos; filtro de conteúdos por perfil de utilizador;

- A manutenção de uma política de *updates* com atualizações verificadas e instaladas automaticamente;

- A manutenção de uma política de *backups* em vigor, bem como toda a documentação relativa aos mesmos;

- Extensão a aplicabilidade dos *backups* a todos os ativos críticos;

- Auditar periodicamente os processos de *backups*;

- Proceder regularmente a reposições de *backups* em ambiente de teste, por forma a garantir que estes são recuperáveis em caso de necessidade;

- A manutenção de uma política de monitorização de acesso a instalações e áreas sensíveis que utilize uma variedade de sistema para se proteger contra perda de dados devido a falhas na fonte de alimentação ou interferências na linha;

- A limitação do acesso às instalações onde os sistemas de informações que tratam os dados de clientes se encontram a indivíduos autorizados e identificados;

- A manutenção de uma política de gestão de acessos que assegure que as informações são compartilhadas com base na necessidade e os utilizadores são identificados de forma exclusiva e em que as exceções são monitorizadas e justificadas;

- A manutenção de registos dos acessos a sistemas e tratamentos de dados do cliente, incluindo o tipo de suportes de dados, o remetente ou destinatários autorizados, data e hora, o número de suportes de dados e os tipos de dados de cliente;

- A política de que nenhum utilizador é administrador e em que função de administrador requer *login* separado;

- A existência de uma política com múltiplas cópias dos Dados do Cliente a partir das quais os dados de clientes podem ser recuperados, com períodos de retenção definidos;

- A implementação de um Processo de gestão de incidentes em que se guarda o registo de todos os incidentes, as responsabilidades são definidas, os procedimentos publicados e existem scripts para gestão de incidentes;

- A eliminação nas bases de dados de toda a informação considerada sensível que não seja necessária à operação;

- A permissão de acessos realizados de fora da rede corporativa apenas através de VPN, cuja atribuição é controlada centralmente;

- A realização de Comunicações entre os hotéis e o *Datacente*r exclusivamente através de túneis VPN seguros;

- A implementação de uma comunicação via correio eletrónico encriptadas com recurso a TLS (*Transport Layer Security*);

- A implementação de uma Política de instalação e atualização de antivírus que cubra a totalidade das máquinas em operação;

- A análise e o levantamento de evidências por parte da direção de informática;

- A preparação modelos de alerta as entidades competentes, bem como o DPO;

- A implementação os mecanismos corretivos necessários, por forma a colmatar as falhas encontradas.

Ao nível dos processamentos manuais de Dados Pessoais foram revistas a seguintes situações:

- A eliminação ou substituição de processos determinados por outros processos automáticos já existentes;

- A formação dos intervenientes para os novos procedimentos;

- A escolha papel e métodos de impressão adequados às condições de armazenamento (período de retenção, humidade ambiente, etc.);

- Quando os documentos são impressos contendo Dados Pessoais estes serem imediatamente recolhidos após a impressão;

- A restrição da distribuição de documentos em papel contendo Dados Pessoais aos indivíduos que os exigem para fins relacionados ao trabalho;

- A guarda em gabinete seguro dos documentos em papel contendo Dados Pessoais (preferencialmente com bloqueio de chave);

- A destruição dos documentos usando uma trituradora;

- A manutenção de um registro específico de todos os documentos que contenham informações pessoais que são enviadas;

- A escolha de canais de transmissão adequados aos riscos e à frequência da transmissão - serviço postal – ou utilizados serviços da organização (veículos e condutores).

As diversas medidas anteriormente implementadas, e as medidas a implementar foram de encontro aos requisitos de segurança do RGPD. Após a análise de risco às infraestruturas informáticas, concluiu-se que estas eram suficientemente robustas para garantir a qualidade dos dados e a deteção de violações, internas ou externas.

Os principais impactos relativamente ao acesso indesejado, a modificações indesejadas ou ao desaparecimento de Dados Pessoais, foram estimados com uma severidade baixa em que os titulares dos dados não são afetados ou em que os inconvenientes são muito reduzidos e ultrapassados sem dificuldades.

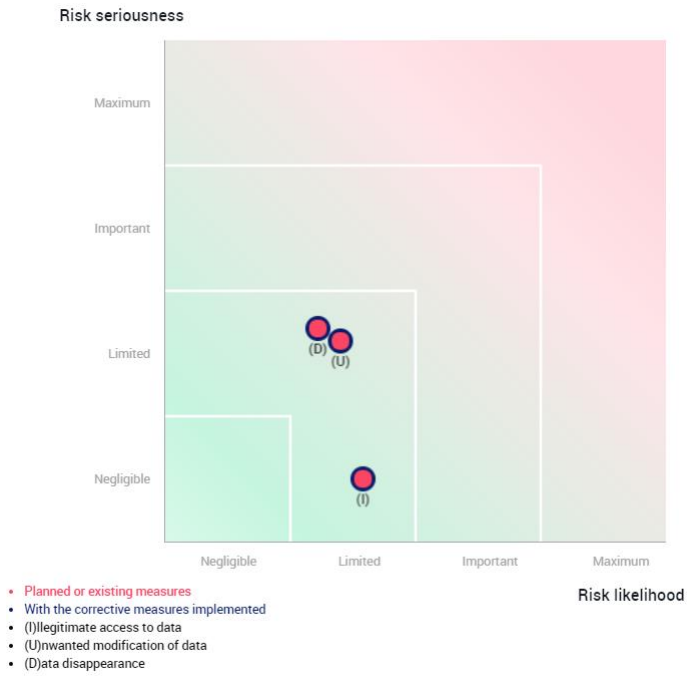

Figura 6 DPIA “Gráfico de projeção de risco” (Fonte Própria, 2018)

Em função da análise realizada, conclui-se que as fontes de risco selecionadas dificilmente se materializariam nas ameaças. As potenciais consequências consideradas são cefaleias temporárias causadas por redundâncias e percas de tempo repetindo formalidades ou aguardando que as mesmas sejam preenchidas ou pelo recebimento de correio eletrónico não solicitado (e.g. *spam*).

Estes incómodos poderão resultar de informações recebidas ou solicitadas, do medo de perder o controlo sobre os dados, o sentimento de invasão de privacidade sem prejuízo

real ou objetivo (por exemplo intrusão comercial) ou em perda de tempo na configuração dos dados. Foi proposto o modelo e a avaliação de risco aos departamentos de administração, jurídico e de tecnologias de informação para validação e posterior publicação.

4.11. Elaboração processo de notificação por violação de dados

O RGPD define como violação de dados como “uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a Dados Pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento”.

Quando uma violação de dados é identificada, o RGPD determina que a documentação a ser fornecida às partes interessadas e à autoridade pública deve conter os factos relacionados com a violação de dados, os efeitos e as medidas corretivas que foram tomadas.

Nos termos do artigo 33.º do RGPD, em caso de violação de Dados Pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos Dados Pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso. O mesmo processo é imposto ao subcontratante perante o responsável pelo tratamento.

A notificação referida deve:

- Descrever a natureza da violação dos Dados Pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de Dados Pessoais em causa;

- Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;

- Descrever as consequências prováveis da violação de Dados Pessoais;

- Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de Dados Pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

A documentação enviada serve para a autoridade de controlo verificar o cumprimento do disposto no RGPD. Para dar resposta a este requisito, foram criados processos e definidos formulários de preenchimento rápido e notificados todos os terceiros, de que, nos termos dos contratos celebrados estão obrigados a prosseguir todos os esforços adequados para auxiliar o hotel no cumprimento da obrigação de notificar a autoridade pública competente e os titulares dos dados sobre uma violação de Dados Pessoais ao abrigo dos Artigos 33º e 34º do RGPD.

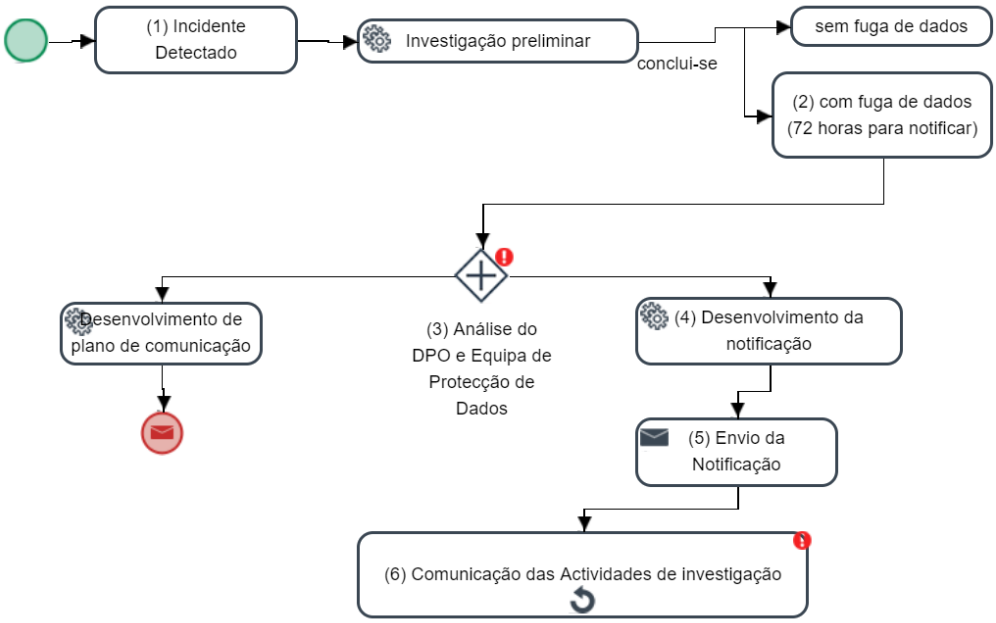

Figura 7 Processo de avaliação de incidentes e de comunicação à CNPD (Fonte Própria, 2018)

De forma a consolidar os processos de notificação, foram propostas ao Departamento de Administração e de Tecnologias de Informação minutas de preenchimento rápido, em caso de necessidade de comunicação (Tabela 13) e desenhados os processos de análise e investigação após a deteção (Figura 7).

Relatório elaborado por: Data: Em nome de:	_____ _____ _____
1. Detalhes da organização (a) Qual é o nome da organização - é o controlador de dados em relação à violação? (b) Quem deve ser contactado para se obter mais detalhes sobre o incidente? (Nome e cargo, endereço de e-mail, número de telefone de contato e endereço)	
2. Detalhes da violação da proteção de dados (a) Por favor, descreva o incidente com o maior detalhe possível. (b) Quando ocorreu o incidente? (c) Como é que o incidente aconteceu? (d) Se houve um atraso na notificação do incidente, quais os motivos; (e) Quais as medidas que a organização aplicou no local para evitar que ocorresse um incidente dessa natureza? (f) Forneça informações relativas às políticas e procedimentos considerados relevantes em vigor no momento em que ocorreu. Forneça as datas em que foram implementadas.	
3. Dados Pessoais colocados em risco (a) Que Dados Pessoais foram colocados em risco? Por favor, especifique se algum dado pessoal financeiro ou sensível foi afetado e forneça detalhes. (b) Quantos indivíduos foram afetados? (c) Os indivíduos afetados estão cientes de que o incidente ocorreu? (d) Quais são as consequências potenciais e adversas. Efeitos para os titulares dos dados? (e) Alguma pessoa afetada reclamou à organização sobre o incidente?	
4. Recuperação (a) * A organização tomou alguma ação para minimizar o efeito sobre os titulares afetados? Em caso afirmativo, forneça detalhes. (b) Os dados colocados em risco agora foram recuperados? Se assim, forneça detalhes de como e quando isso ocorreu. (c) Quais as etapas para prevenir a reincidência desse incidente?	
5. Formação e orientação (a) Que formação é oferecida aos funcionários sobre os requisitos da Lei de Proteção de Dados?	
6. Contato prévio com a CNPD (a) Existem incidentes anteriores comunicados à CNPD nos últimos dois anos? (b) Se a resposta à pergunta acima for sim, forneça detalhes breves	
7. Diversos (a) Outras notificações sobre esse incidente. (b) Tem havido cobertura mediática do incidente? Se assim, forneça detalhes.	

Tabela 13 “Minuta de comunicação à CNPD” (Fonte Própria, 2018)

4.12. Notificação da Comissão Nacional de Proteção de Dados de Transferências de Dados Pessoais

A notificação à Comissão Nacional de Proteção de Dados a que nos referimos neste subcapítulo, é diferente daquela que abordámos no subcapítulo anterior relativa a violação de Dados Pessoais. Nos termos do artigo 44.º do RGPD "qualquer transferência de Dados Pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro (...) só é realizada" se determinadas condições estabelecidas no Regulamento forem respeitadas pelo responsável pelo tratamento e pelo subcontratante.

As cadeias hoteleiras que disponham de unidades fora do espaço europeu, e que nelas queiram utilizar Dados Pessoais de cidadãos europeus estão sujeitas a estas regras. As transferências internacionais de dados podem realizar-se através mecanismos que tenham "em conta se o país de destino dos dados assegura ou não um nível de proteção adequada"[82]. Para que os hotéis possam transmitir os Dados Pessoais dos seus clientes para outras unidades fora da União existem duas possibilidades. A primeira assenta em transferir os Dados Pessoais para os países que constam da lista da Comissão publicada no *Diário Oficial da União Europeia* em relação aos quais se tenha decidido que se garante um nível de proteção adequado. À falta de decisão de adequação da Comissão, o hoteleiro apenas poderá transmitir os Dados Pessoais para um país terceiro se tiver apresentado à autoridade de controlo as garantias adequadas. Estas podem consistir em[83]: instrumentos juridicamente vinculativos entre as empresas e as autoridades públicas; contratos denominados de *Binding Corporate Rules; ou,* cláusulas-tipo de proteção de dados adotadas pela Comissão.

Nos termos da "Deliberação n.º1770/2015 relativa ao procedimento de análise dos Acordos Intragrupo para transferências de dados para fora da União Europeia da Comissão Nacional de Proteção de Dados" as transferências de Dados Pessoais para fora da União Europeia têm aumentado de forma expressiva, "acompanhando os novos modelos de negócio e o dinamismo das relações comerciais numa economia crescentemente globalizada".

De forma a cumprir os requisitos constantes no artigo 47.º do RGPD, foram preparados durante a implementação do Regulamento, contratos com cláusulas-modelo de contrato e propostas de comunicação à CNPD das regras corporativas vinculativas que protegem

[82] Nos termos da "Deliberação n.º1770/2015 relativa ao procedimento de análise dos Acordos Intragrupo".

[83] Yáñez, S. (2017). *Data Protection Officer - JusJornal, N. º 15, Secção Proteção de dados*. Alphen aan den Rijn: Wolters Kluwer

as transmissões de dados internacionais dentro do âmbito da empresa. Estes contratos multilaterais entre empresas do mesmo Grupo, designados por Acordos Intragrupo, são considerados adequados desde que "sejam idênticos e se encontrem em conformidade com as cláusulas contratuais-tipo aprovadas pela Comissão Europeia"[86].

Nos mesmo sentido, foram revistos os termos contratados de forma a demonstrar que os contratos de prestação de serviço consubstanciaram o mesmo mecanismo de proteção de transferência de dados dentro dos seus grupos empresariais uma vez que as empresas que prestam este tipo de serviços optam genericamente por maximizar os fluxos de processamento e de acesso aos dados e utilizam diversos servidores ao mesmo tempo em localizações díspares.

Com o processo de notificação à CNPD ficou concluída a fase inicial de implementação do Regulamento Geral de Proteção de Dados.

[86] Nos termos da Deliberação n.º 1770/2015 relativa ao procedimento de análise dos Acordos Intragrupo

Conclusão

Reflexão e análise Geral do Estágio

O gestor hoteleiro tem como principais funções coordenar e dirigir a atividade dos vários departamentos dos hotéis de forma a garantir um bom funcionamento da empresa, a satisfação dos clientes e a consolidação dos interesses da administração e dos proprietários. A estrutura deste estágio em modelo de *cross-training* permitiu compreender a importância individual de cada departamento, a relação dinâmica entre os vários departamentos e a performance geral. A implementação do Regulamento Geral de Proteção de Dados obrigou a um estudo dos dados de negócio e dos fluxos de informação no seio da empresa e a uma relação de confiança que contribuiu para uma visão muito abrangente da gestão.

O primeiro objetivo específico deste estágio foi interpretar o novo Regulamento Geral de Proteção de Dados Pessoais, enumerar os requisitos legais substanciais e formais impostos e as boas práticas sugeridas às empresas. De forma a dar resposta a este objetivo foram consultadas as versões portuguesa e inglesa dos textos do Regulamento e os textos complementares do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados relativo aos guias de trabalho para o DPO e as orientações relativas à Avaliação de Impacto sobre a Proteção de Dados que determinam se o tratamento é suscetível de resultar num elevado risco, o Grupo de Trabalho do Artigo 23 relativo aos propósitos das limitações do tratamento e foram mantidos contactos regulares com o Departamento Jurídico e com a Administração de forma a validar as interpretações jurídicas dos pontos em análise. Participei em conferências, fóruns e reuniões de trabalho de forma a aprofundar os conhecimentos em relação ao tema, nomeadamente, na conferência "*Beyond – Portugal Digital Revolutions*", promovido pela EY Portugal, na Fundação Calouste Gulbenkian a 17 de outubro de 2017, na Acão de formação "Regulamento Geral de Proteção de Dados", promovida pela Ordem dos Advogados em Lisboa a 3 de maio de 2018, e em reuniões de trabalho com a Microsoft Portugal e outros especialistas da área da segurança informática.

O segundo objetivo foi compreender e caracterizar a natureza e os fluxos de informação dentro da empresa, a estrutura, as funções e as relações entre os diversos departamentos centrais, e entre estes e os hotéis. De forma a dar resposta, foram mantidos contactos regulares com os vários departamentos dentro do grupo e preenchidos diversos inventários relativos aos documentos utilizados para a recolha e armazenamento de dados.

O terceiro objetivo foi desenvolver e implementar um conjunto de medidas que garantissem a conformidade de todas as operações de tratamento de Dados Pessoais com os requisitos impostos pelo RGPD. O processo de desenvolvimento de conformidades dependeu do entendimento dos diversos departamentos em relação às diversas opções propostas e a implementação respeitou os tempos previstos.

Limitações do trabalho

Como referimos anteriormente, implementar um regulamento como o RGPD, é um processo que consume tempo e recursos à operação hoteleira, com impactos consideráveis nos processos, no desempenho dos sistemas de informação e nas atividades dos diversos departamentos.

Do ponto de vista estrutural, o RGPD é uma mudança de paradigma de gestão em que a proteção da privacidade passa de um modelo de hétero-regulamentação para um modelo de autorregulamentação. No momento em que procedemos à conceção das medidas, não existiam quaisquer modelos de *benchmarking* e a resolução de questões foi realizada sobretudo em função de soluções pensadas caso a caso ou analogamente. Este foi um aspeto muito entusiasmante do projeto, mas que ao mesmo tempo pode ter limitado o seu desenvolvimento. Por exemplo, o facto de não existirem disponíveis no mercado modelos validados para a realização de Avaliação de Impacto da Privacidade de Dados, independentemente dos contactos realizados juntos da Comissão de Nacional de Proteção de Dados, obrigou ao desenvolvimento de um modelo não testado e concebido de raiz.

Por outro lado, algumas questões jurídicas carecem de desenvolvimentos e esclarecimentos futuros, esclarecimentos que apenas poderão advir da prática jurídica continuada, da litigância, da jurisprudência e da doutrina que venha a ser produzida. Por exemplo, a utilização massiva de contactos de correio eletrónico para ações de marketing que poderá sugerir que os endereços de correio eletrónico venham a ser considerados dados “sensíveis” pelo seu potencial fraudulento.

Do ponto de vista temporal, a limitações ao nível da implementação, prenderam-se com a necessidade de ajustamento dos processos do RGPD ao sector da hotelaria, a falta de recursos especializados no mercado num momento em que os prestadores de serviços ainda estão a desenvolver produtos para dar resposta às questões relativas à Privacidade e ao RGPD e o tempo necessário para contrariar as barreiras à mudança dentro das organizações.

As principais vantagens para a execução deste projeto foram o facto de o sistema de gestão (ERP) ser desenvolvido por profissionais dentro da empresa e o facto dos administradores e dos funcionários terem um conhecimento profundo do negócio e da actividade hoteleira

De forma a validar os processos e as medidas tomadas no decorrer da implementação foi realizada uma consulta externa. De acordo com os consultores contratados a abordagem seguida pelas propostas foi considerada muito positiva, e até conservadora, no sentido em que foram adotadas medidas que vão além do exigido pelo Regulamento.

Medidas sugeridas para o futuro

Com a aplicação continuada do Regulamento existirão certamente questões a aprofundar e a desenvolver.

Algumas medidas futuras a implantar poderão passar por:

- Contratar coberturas de proteção que permitam segurar os prejuízos decorrentes das violações de privacidade (peritos, advogados e serviços de relações públicas que oferecem resposta rápida perante os eventos). Alguns dos produtos já disponíveis no mercado oferecem inclusivamente serviços com vista à reparação da reputação, monitorização de custos, a recuperação e recolha de dados;

- Considerar alternativas a subcontratantes norte-americanos, passando a contratar subcontratantes europeus. Apesar de os subcontratantes contratados estarem certificados ao abrigo do *Privacy Shield* - o que se traduz em garantias – com subcontratantes europeus os dados não serão, em princípio, transferidos para fora da União Europeia;

- Rever periodicamente os *logins* internos de modo a reforçar a rastreabilidade das ações dos colaboradores sobre os Dados Pessoais de clientes e a avaliar o seu nível de fiabilidade em termos de segurança;

- Analisar periodicamente as bases de dados na perspetiva de guardar apenas os dados necessários e pelo menor tempo possível;

- Preparar alterações ao portal de clientes nas diversas línguas (português, francês, espanhol e alemão) tendo em atenção a terminologia usada no Regulamento nesses idiomas;

- Desenvolver em formato de academia *online* uma ferramenta de aprendizagem de forma a disponibilizar a informação relativa à proteção de dados a todos os colaboradores de modo imediato independentemente da localização geográfica;

- Preencher periodicamente listas de avaliação e de revisão nas diversas unidades de modo a incluírem apenas os dados estritamente necessários.

Para além destas medidas, será aconselhável realizar testes de invasão ou *phishing* de forma a analisar o nível de segurança do sistema tecnológico, a capacidade de reação dos colaboradores e a aplicação do manual de normas. Estes testes normalmente envolvem aplicações enviadas por correio eletrónico com o propósito de obter o acesso ao sistema, desta forma, conseguem-se mapear as vulnerabilidades e os pontos fracos do sistema e reforçar os pontos-chave da formação de segurança realizada junto dos colaboradores.

Por último, poderá desenvolver-se um Manual de Normas específico para o Departamento de Marketing onde se espelhem as questões e consequências do RGPD para as suas atividades e funções, nomeadamente, na contração das bases de dados, no novo limite de alcance de determinados canais de promoção e no custo do *pay per click*.

Bibliografia

Avignon, C. (2016). *La décision d'adéquation pour l'EU-US Privacy Shie*ld. Disponível em alain-bensoussan.com

Batenman, S. (1998). Administração: Construindo Vantagem Competitiva. São Paulo: Atlas

Bennett, Colin J. (1992). *Regulating Privacy.Data Protection and Public Policy in Europe and the United State*. Ithaca: Cornell University Press.

Brown R., (2017, 7 Agosto). *UK consumers will be able to force social media giants to delete embarrassing posts under new data law*. Consultado em janeiro 15, 2018 em https://www.cnbc.com/2017/08/07/uk-consumers-to-have-right-to-be-forgotten-under-data-protection-law.html

Cavoukian, A. (2009). Privacy by Design, The 7 Foundational Principles". Canada: Information and Privacy Commissioner of Ontario.

Correia, V. (2014). Sobre Direito à Privacidade. In Miranda, J. *O Direito* (240 p). Lisboa: Editora Almedina.

Cruz, G., & Gâmdara, J. M. G (2003). O turismo, a hotelaria e as tecnologias digitais. *Revista Turismo Visão e Ação,* Vol.5. Disponível em http://siaiweb06.univali.br/seer/index.php/rtva/article/viewFile/1135/898

De Bos, T. (2018), *GDPR Today & Tomorrow, how to create a sustainable GDPR implementation?* Consultado em maio 15, 2018 em https://consulting.ey.com/ready-eus-new-general-data-protection-regulation/

Greenberg, P. (2001). RM at the Speed of Light. Londres: Addison-Wesley Professional.

Hespanha, P. (2000). Entre o estado e o mercado. As fragilidades das instituições de proteção social em Portugal. Coimbra: Quarteto.

KPMG (2017). *O Impacto do Regulamento Geral de Proteção de Dados em Portugal.* Consultado em outubro 5, 2017 em https://assets.kpmg.com/content/dam/kpmg/pt/pdf/pt-2017-rgpd.pdf

Instituto Nacional de Estatística (2018). Resultados preliminares de 2017: crescimentos de 8,9% nos hóspedes e 7,4% nas dormidas. Consultado em março 15, 2018 em https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=281091107&DESTAQUESmodo=2

Mayer-Schonberg, V. (2001). General Development of Data Protection in Europe, in *AGRE, Philip E. e Rotenberg, Marc – Technology and Privacy: The New Landscape*. Londres e Massachussetts: MIT Press.

Oliveira A. (2002). A reserva da intimidade da vida priva e familiar. In *Revista da Faculdade de Direito da Universidade de Lisboa* (Vol. XLIII-Nº1, p. 14). Lisboa: Coimbra Editora.

Oliveira, P. (2012, fevereiro 1). *ERP's na Hotelaria.* Consultado em maio 6, 2018 em http://hotelarianacional.blogspot.pt/2012/02/erps-na-hotelaria.html

Pinheiro, A. S. (2012) *A proteção de dados na proposta de regulamento comunitário apresentada pela Comissão Europeia: primeiras reflexões* (p 9 e 10). Lisboa: Diário de Bordo

Pinheiro, A. S. (2012). A Proteção de Dados na proposta de regulamento comunitário apresentada pela Comissão Europeia primeiras reflexões. In *Direito e Política* (Out. 2012, pp. 09- 21.). Lisboa: Diário de Bordo.

Pinheiro, A. S. (2015). *Privacy e proteção de Dados Pessoais: a construção dogmática do direito à identidade informacional* (908 p.). Lisboa: AAFDL.

Portal do Cidadão. A CNPD. Disponível em https://www.portaldocidadao.pt/web/comissao-nacional-de-protecao-de-dados/comissao-nacional-de-protecao-de-dados

PWC (2018, fevereiro 2*). "Using Personal Data to Build Customer Trust and Competitive Advantage*. Consultado em maio 3, 2018 em http://pwc.blogs.com/analytics_means_business/2017/02/using-personal-data-to-build-customer-trust-and-competitive-advantage.html

Yáñez, S. (2017). *Data Protection Officer - JusJornal, N.º 15, Secção Proteção de dados* / Temas de hoje. Alphen aan den Rijn: Wolters Kluwer

Teixeira, M. L. S. (2013). A União Europeia e a Proteção de Dados Pessoais – "Uma visão futurista". In *Revista do Ministério Público*. (Jul. – Set. 2013 p. 65-106). Lisboa: Sindicato dos Magistrados do Ministério Público.

Torres, C. (2016). *Les BCR sous-traitants, un instrument d'encadrement des flux*. Disponível em alain-bensoussan.com

Vila Galé. *Media Kit.* Consultado em março 15, 2018 em https://www.vilagale.com/pt/grupo/media-kit

Legislação e Jurisprudência

Pacto Internacional sobre os Direitos Civis e Políticos e Protocolos Facultativos. In Bacelar Gouveia, J. (2009). *Direito Internacional Público - Textos Fundamentais*. Editora: Coimbra

Constituição da República Portuguesa (Coimbra: Almedina, 2002)

Lei n.º 67/98. Lei da Proteção Dados Pessoais (transpõe para a ordem jurídica portuguesa a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à proteção das

pessoas singulares no que diz respeito ao tratamento Dados Pessoais e à livre circulação desses dados.

Parlamento Europeu e do Conselho. Regulamento (UE)) 2016/679 do Parlamento Europeu e do conselho de 27 de abril de 2016. *Regulamento Geral de Proteção de Dados*. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

Tribunal de Justiça da União Europeia. *Processo n.º C-73/07*. Consultado em 12 Dezembro 2017 em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd52ff4da201ef4b0d8c7a8875e96eb2f7.e34KaxiLc3qMb40Rch0SaxuQa310?text=&docid=76075&pageIndex=0&doclang=PT&mode=lst&dir=&occ =first&part=1&cid=666398