INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE LISBOA


# A AUDITORIA E A PROTEÇÃO DE DADOS DOS CONSUMIDORES DE ALOJAMENTO LOCAL

Mariana Teodoro da Silva

Lisboa, julho de 2021

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

# A AUDITORIA E A PROTEÇÃO DE DADOS DOS CONSUMIDORES DE ALOJAMENTO LOCAL

Mariana Teodoro da Silva

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sob a orientação científica do Professor Doutor Fernando J L Rodrigues, Professor Adjunto e Docente de Carreira da Área científica de Informática do ISCAL.

Constituição do Júri:

Professor Especialista Gabriel Correia Alves - Presidente

Professora Especialista Maria da Luz Miranda - Arguente

Professor Doutor Fernando João Rodrigues - Vogal

Lisboa, julho de 2021

Declaro ser a autora desta dissertação que constitui um trabalho original e inédito, que nunca foi submetido (no seu todo ou qualquer das suas partes) a outra instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas. Mais acrescento que tenho consciência de que o plágio – a utilização de elementos alheios sem referência ao seu autor – constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação. O presente trabalho respeita as normas vigentes no Manual para elaboração de dissertações do ISCAL (e especificamente norma americana para referenciação bibliográfica *American Psychological Association* – APA) e o texto respeita a ortografia pré-acordo (algumas citações) e pós-acordo ortográfico.

## Agradecimentos

A concretização desta dissertação não seria possível sem o apoio e a cooperação de um conjunto de pessoas às quais não poderia deixar de agradecer.

Quero agradecer ao meu orientador, o Professor Doutor Fernando Rodrigues, por ter estado do meu lado literalmente até ao último instante, pela enorme paciência que teve, por todas as orientações e conselhos que me deu. Sem ele a conclusão deste projeto seria impossível.

À minha família, pelo apoio incondicional e permanente, por me terem dado todas as bases e todas as ferramentas que me permitiram chegar até aqui, por nunca desistirem de mim e não me deixarem desistir dos meus sonhos e objetivos mesmo quando parecem impossíveis ou inalcançáveis.

Por fim, ao meu namorado pela compreensão da minha ausência e falta de tempo destes últimos meses e por todo o apoio e acompanhamento neste final de mais uma etapa.

## Resumo

Com a eclosão da Internet, diversas organizações, aventuraram-se na expansão dos seus negócios através das novas tecnologias, motivo que, contribuiu para o desenvolvimento em escala do Alojamento Local (AL).

Simultaneamente o Regulamento Geral sobre a Proteção de Dados (RGPD) veio modificar a forma como as organizações geriam os dados pessoais dos seus consumidores, estabelecendo quais os requisitos mínimos para o seu tratamento, de modo a garantir os direitos e liberdades das pessoas singulares.

Nos dias de hoje, com um número incalculável de transações diárias de dados pessoais, torna-se inadiável, avaliar a seguridade e fiabilidade do AL no que respeita aos dados pessoais dos seus consumidores e sob que formas estes são tratados.

Perante os distintos contextos de risco e procedimentos específicos inerentes à atividade deste setor, o principal objetivo de estudo, passa por identificar os mecanismos e procedimentos adotados na atividade do AL face ao RGPD, com base nos dados recolhidos a partir de um questionário dirigido a profissionais que laboram diretamente nesta área de negócio.

O presente estudo reflete, com base nos resultados obtidos, o paradigma da diminuta perceção que as organizações de AL possuem acerca do RGPD e da escassez de procedimentos adotados. Estes fatores evidenciam a necessidade de intervenção e acompanhamento contínuo por parte da Auditoria, bem como, da criticidade de auditar a aplicabilidade destes procedimentos e do seu cumprimento tendo por base os requisitos impostos pela legislação vigente.

Neste sentido, a opção apresentada como «Considerações Finais» indica que o resultado do trabalho de investigação possibilita reflexões, sem uma conclusão definitiva.



Palavras-chave: Alojamento Local, Auditoria, Proteção de Dados; Regulamento Geral da Proteção de Dados da União Europeia (RGPD), Sistemas de Informação (SI).

## *Abstract*

*With the outbreak of the Internet, several organizations ventured into the expansion of their business through new technologies, which contributed to the development of Local Accommodation (LA) at scale.*

*At the same time, the General Data Protection Regulation (GDPR) has changed the way organizations manage their consumers' personal data, establishing the minimum requirements for their processing to guarantee the rights and freedoms of natural persons.*

*Nowadays, with an incalculable number of daily transactions of personal data, it becomes in deferred, to assess the security and reliability of LA about the personal data of its consumers and in what ways they are processed.*

*Given the different risk contexts and specific procedures inherent to the activity of this sector, the main objective of the study is to identify the mechanisms and activities adopted in the activity of LA face to the GDPR, based on the data collected from a questionnaire addressed to professionals who work directly in this business area.*

*The present study reflects, based on the results obtained, the paradigm of the small perception that LA organizations have about the GDPR, and the scarcity of procedures adopted. These factors highlight the need for intervention and continuous monitoring by the Audit, as well as the criticality of auditing the applicability of these procedures and their compliance based on the requirements imposed by the current legislation.*

*The option presented as "Final Considerations" indicates that the result of the research work enables reflections, without a definitive conclusion or a result susceptible to revisions.*



*Keywords: Local Accommodation, Auditing, Data Protection; General Data Protection Regulation of the European Union (RGPD), Information Systems.*

# Índice

## Índice de Gráficos

## Índice de Figuras

## Índice de Tabelas

## Lista de abreviaturas e siglas

| | |
|---|---|
| AF | Auditoria Financeira |
| AHRESP | Associação da Hotelaria, Restauração e Similares de Portugal |
| AI | Auditoria Interna |
| AIPD | Avaliação de Impacto sobre a Proteção de Dados |
| AL | Alojamento Local |
| ASI | Auditoria de Sistemas de Informação |
| AEPD | Autoridade Europeia para a Proteção de Dados |
| CDE | Conselho da Europa |
| CEDH | Convenção Europeia dos Direitos do Homem |
| CM | Câmara Municipal |
| CNPD | Comissão Nacional de Proteção de Dados |
| CNPDPI | Comissão Nacional de Proteção de Dados Pessoais Informatizados |
| CRP | Constituição da República Portuguesa |
| CT | Código do Trabalho |
| DPO | *Data Protection Officer* |
| EPD | Encarregado de Proteção dos Dados |
| IoT | Internet of Things (Internet das Coisas) |
| IVA | Imposto sobre o Valor Acrescentado |
| IRC | Imposto sobre o Rendimento de Pessoas Coletivas |
| PD | Proteção de Dados |
| RNT | Registo Nacional de Turismo |
| RGPD | Regulamento Geral de Proteção de Dados |
| SEF | Serviço de Estrangeiros e Fronteiras |
| SI | Sistemas de Informação |
| TI | Tecnologias de Informação |
| TIC | Tecnologias da Informação e da Comunicação |
| TEDH | Tribunal Europeu dos Direitos do Homem |
| UE | União Europeia |

# Introdução

Desenvolvida no âmbito do Mestrado em Auditoria, a presente dissertação, visa apresentar como tema de investigação «**A Auditoria e a Proteção de Dados dos Consumidores de Alojamento Local**».

Incide, sobre o estudo e análise dos procedimentos adotados pelas organizações de AL, evidenciando a importância e aplicabilidade da auditoria, face a duas temáticas relativamente recentes: o Alojamento Local (AL) e a Proteção de Dados (PD).

Pretendeu-se, com base nas respostas obtidas num questionário dirigido a profissionais da área, investigar a adoção e o cumprimento do RGPD na área do AL e evidenciar o papel da Auditoria através de um conjunto diversificado de contributos para a monotorização e realização de auditorias no setor do AL, por forma a atestar a fiabilidade do tratamento e gestão de dados pessoais no âmbito da aplicabilidade e cumprimento do RGPD.

## 1.1 Breve Enquadramento e Relevância do Tema

Embora sem conexão aparente entre o AL e a PD, estes distintos temas, têm vindo a despertar debates por todo o mundo com as suas diversas reformas legislativas.

Alvos de constantes transformações no decorrer dos últimos anos, atualmente, tanto o AL como a PD, integram o conjunto de temas presentes na agenda política europeia.

O AL veio inovar o processo de expansão das cidades, sobretudo ao nível das capitais europeias, que têm superado inúmeras reabilitações urbanas para fazer face à procura crescente de turismo. Não só as reabilitações urbanas requerem atenção, também o célere desenvolvimento dos Sistemas de Informação (SI) necessita de ser reavaliado, uma vez que representa grande parte do crescimento do turismo e cuja utilização requer da introdução de inúmeros dados pessoais por parte dos consumidores.

Aliado à problemática da privacidade e da proteção de dados, que tem vindo a adquirir especial interesse, surgiu a necessidade de legislar, perante o cenário do direito, um regulamento que viesse uniformizar os direitos e liberdades considerados fundamentais de cada cidadão.

Resultante da utilização imprópria e do aproveitamento generalizado de dados pessoais, a União Europeia, publicou no ano de 2016 o Regulamento Geral sobre a Proteção de Dados (RGPD). A publicação deste regulamento resultou da necessidade de introduzir diretrizes capazes de regulamentar a proteção de dados no que concerne à recolha e ao tratamento de dados de pessoas singulares e à livre circulação dos mesmos.

Perante este contexto de transformação, a elaboração do presente estudo, trata um tema relativamente recente e pouco desenvolvido, com o propósito de aferir a aplicabilidade e o cumprimento do RGPD nas organizações de AL e o papel que a auditoria pode desempenhar como ferramenta de apoio à implementação e correta adoção do RGPD.

Pese embora as grandes generalidades destas entidades se caracterizem como micro ou pequenas empresas e ainda que não estejam obrigadas a algumas das especificidades estatuídas no RGPD não é possível descredibilizar os enormes volumes de dados pessoais que operam diariamente nem os riscos que daí sucedem.

Importa por isso destacar o interesse e o papel dos auditores, bem como, a necessidade de atuação da auditoria perante a problemática do RGPD no AL, através de mecanismos de monotorização que poderão ser capazes de mitigar esta lacuna existente na aplicabilidade e no cumprimento deste regulamento.

## 1.2 Objeto e Objetivos do Estudo

Numa economia fundamentalmente apoiada nos novos procedimentos tecnológicos, revela-se necessário, analisar o modo como o AL tem vindo a evoluir e a atuar, sobretudo ao nível da proteção de dados pessoais.

É, portanto, neste contexto, que o objeto de estudo desenvolvido na presente dissertação tem como fundamento o RGPD no AL onde é pretendido identificar, compreender e relacionar quais os mecanismos adotados no que diz respeito à proteção de dados dos consumidores.

Verificar o cumprimento dos requisitos impostos pelo RGPD, apresentar as problemáticas existentes e compreender através de mecanismos de monotorização se estas organizações estão aptas a lidar com dados pessoais.

A visão a ser analisada, bem como, as reflexões que se pretendem alcançar, vêem-se também fundamentadas pelo volume de dados disponibilizados às organizações de AL relativamente à proteção dos dados pessoais e ao estatuído no RGPD.

Deste modo, **a questão de partida** para este estudo e à qual se pretende obter resposta é: "Passados dois anos desde a aprovação do RGPD estarão as organizações de AL a cumprir com os critérios indicados por este regulamento ou necessitarão de apoio por parte da auditoria?"

Em termos científicos e com o intuito de responder à questão central o principal objetivo é dar a conhecer as políticas e os procedimentos adotados nas empresas de AL no que respeita à proteção de dados pessoais e ao RGPD e consequentemente, fornecer matéria para investigações futuras.

Tendo em consideração que a grande maioria das empresas de AL não se encontram obrigadas à aplicabilidade de algumas das especificidades impostas pelo RGPD, mas tratam de modo direto e diário inúmeros dados pessoais, do ponto de vista social pretende-se, ao nível da segurança e privacidade da informação, alertar para a importância da aplicabilidade e do cumprimento do estatuído neste regulamento e avaliar a sua aplicabilidade nos dias de hoje.

Em termos práticos, pretende-se evidenciar para a importância da auditoria e da sua intervenção neste processo de melhoria e de controlo ao nível da aplicabilidade e do cumprimento do RGPD nestas organizações fornecendo mecanismos de monotorização capazes de corresponder às diferentes necessidades intrínsecas à atividade do AL.

## 1.3 Metodologia Geral

A metodologia adotada para a presente dissertação, teve inicialmente por base uma pesquisa bibliográfica e documental com o intuito de investigar e compreender, a evolução histórica da auditoria nas suas diferentes vertentes e a evolução legislativa do AL e do RGPD, face às antecedentes legislações nacionais e europeias, permitindo depreender os impactos obtidos no quadro jurídico da proteção de dados pessoais, após os dois primeiros anos de implementação.

Nesta fase inicial de revisão literária e tendo em conta se tratar de temas relativamente recentes e pouco abordados, deu-se especial atenção para artigos e revistas científicas, assim como, para legislação nacional e internacional sobre os temas em análise.

A obtenção de resultados fidedignos, é um dos objetivos fulcrais com que se rege a presente dissertação, motivo pelo qual foram combinadas as várias fontes de dados supracitadas.

Posteriormente na componente prática a metodologia investigacional adotada teve por base a elaboração de um inquérito por questionário, composto por uma composição de questões simples, dirigida a sócios e colaboradores de empresas de AL sediadas em território nacional, que tratam dados pessoais, com o intuito de aferir quais os procedimentos adotados face à política de proteção de dados e avaliar se as organizações em estudo estão em observância com as exigências impostas pelo RGPD.

Os dados recolhidos foram utilizados para uma análise descritiva simples como forma de aferir os processos de recolha, tratamento e partilha de dados pessoais no sector do AL, permitindo evidenciar áreas e matérias de risco e fornecer ferramentas de controlo que consintam fazer face aos possíveis riscos evidenciando contributos para a monotorização da aplicabilidade e cumprimento do RGPD.

## 1.4 Estrutura da Dissertação

A presente dissertação está subdividida em cinco capítulos. No primeiro capítulo é apresentado, para além da estrutura, o tema, a problemática da investigação e a sua relevância, assim como o objeto, os objetivos, a metodologia de investigação adotada.

O segundo capítulo é dedicado à revisão de literatura relacionada com a Auditoria, o Alojamento Local e a Proteção de Dados, onde é pretendido analisar com base numa perspetiva teórica, a evolução histórica e legislativa destes temas por forma a enquadrar a relevância e o interesse do tema.

Complementarmente, no terceiro capítulo é feita uma descrição relativamente à metodologia adotada e é apresentada a análise efetuada sobre o processo de recolha de dados obtidos através de um inquérito por questionário, dirigido a utilizadores que laboram diretamente na área do AL e tratam e/ou armazenam dados pessoais.

Este capítulo compreende também a caracterização da população e amostra em estudo, o período de recolha e as hipóteses em análise, bem como, são apresentados e interpretados os resultados obtidos no inquérito realizado.

Tendo em consideração que a esmagadora maioria das empresas que compreendem o setor de AL não estão obrigadas a auditoria externa nem possuem auditoria interna serve o quarto capítulo para evidenciar a necessidade de reajustar este paradigma no que diz respeito ao tratamento de dados pessoais no setor do AL.

Por esse motivo, o quarto capítulo contempla e com base na importância associada à temática da proteção de dados e nos resultados obtidos e interpretados no capítulo anterior, um conjunto de contributos, baseados na atividade de auditoria e especificamente adaptados à atividade do AL, para a monitorização e melhoramento dos procedimentos analisados em estudo.

Por último, o quinto capítulo contém as considerações finais e respetivas limitações associadas à investigação realizada e evidencia a importância do papel da auditoria no apoio para a implementação e controlo dos mecanismos internos a adotar pelas empresas deste setor no que respeita à proteção de dados e ao RGPD. Este capítulo identifica ainda temas/áreas para futuras investigações que se revelam ao longo do estudo impactantes a nível económico e social e conferem por isso especial interesse em aprofundar.

# 2 Enquadramento Teórico

## 2.1 A Auditoria

Os serviços de auditoria possuem um claro interesse público e têm passado por diferentes épocas de crise financeira e de credibilidade a nível social.

Primordialmente a auditoria de acordo com Pixley (1881 citado por Chambers[1], 1995, p. 75) e Bourne (1887 citado por Chambers[2], 1995, p.75) tinha como propósito detetar erros, perpetrados pelas empresas, sobretudo erros de *«[…] omission; […] commission; […] principle*» mas também reconhecer e prevenir situações de fraude, nomeadamente, «[…] *where it has been committed, and its prevention by imposing such safeguards and devising such means as will make it extremely difficult accomplishment*».

De um modo concordante, também Holmes (1956, p.1) contextualizou o propósito da auditoria, denominada como Auditoria Financeira (AF) ou externa, como «[…] *ascertain the accuracy, integrity and authenticity of those statements, records, and documents*».

Contudo, face à crise financeira de 2008 que o mundo atravessou, as empresas sentiram a necessidade de prestar informação financeira, não só mais equiparável como mais credível e para tal, requeriam dos serviços prestados pelos auditores.

Na opinião de Arens, Elder e Beasley (2003, p.4) o trabalho desenvolvido pelos auditores determina-se como «[…] *the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria*».

Com o gradual aumento dos mercados financeiros, a auditoria revelou-se importante para a consolidação da influência empresarial e para garantir credibilidade nas demonstrações financeiras, facto que, contribuiu para o aparecimento de uma nova visão sobre o conceito da mesma, na medida em que o principal objetivo deixou de ser a deteção da fraude, mas sim, asseverar a informação contida nas demonstrações financeiras.

[1] Pixley, F. W. (1881). *Auditors: their duties and responsibilities*. London: Effingham Wilson

[2] Bourne, J. H. (1887). *Acct*

Esta nova visão, vai ao encontro com a definição dada por Stamp e Moonitz (1978 citado por Costa[3], 2017, p.59), em que caracterizam a auditoria como «[…] um exame independente, objetivo e competente de um conjunto de demonstrações financeiras de uma entidade, juntamente com toda a prova de suporte necessária» tendo como intuito «a intenção de exprimir uma opinião informada e fidedigna, através de um relatório escrito, sobre se as demonstrações financeiras apresentam apropriadamente a posição financeira».

Já a American Accounting Association (AAA) (1973, p.2) avalia a auditoria como um

> […] "*systematic process of obtaining and objective evaluation of the evidence referring the statements regarding documents or events with economic character in order to appreciate the degree of conformity of these with pre-established criteria, to communicate the results of the interested parts"*.

O início do estudo ao nível do conhecimento da auditoria em diversas áreas, aliado em simultâneo, com a expansão das Tecnologias de Informação (TI), que têm vindo a desenvolver-se ao longo do tempo, permitiu, de igual modo, acrescentar novos valores à visão da auditoria, reformulando por consequência também a sua missão. Contrariamente ao que se sucedia, atualmente, a Auditoria Financeira (AF) é ainda uma das vertentes mais relevantes, mas não única, da auditoria como um todo.

Perante a importância da AF, surgiu a necessidade de instituir outras auditorias tais como a Auditoria Interna, Previsional, Operacional, Forense, de Conformidade, Auditoria a Sistemas de Informação e muitas outras, onde são diversas as normas empregues na apreciação das mesmas que refletem sobre diversos aspetos, em particular, ao objetivo, à extensão, à constância, à substancialidade e ainda ao indivíduo que as concretiza.

Em preceito, uma auditoria integra-se, sempre, em numerosos critérios apreciativos, onde subsistem diferentes tipos de auditorias, que exigem funções distintas e que aliadas, resultam na credibilização da informação financeira e não financeira relevante para a tomada de decisão, mas sobretudo para acrescentar valor às organizações.

[3] Stamp, E. & Moonitz, M. (1978). *International Auditing Standards*. London: Prentice Hall.

## 2.2 A Auditoria Interna

A impossibilidade de analisar a totalidade dos procedimentos existentes numa Organização, revelou-se ao longo do tempo, evidente razão pela qual, foi necessário instituir normas e procedimentos internos, capazes de dar resposta ao desenvolvimento organizacional.

Inestimáveis, são as suscetibilidades financeiras inseridas na economia universal, que conduzem à relevância crucial do papel da auditoria e dos auditores na sociedade, como instrumento de transparência, independência e fiabilidade no apoio aos órgãos de gestão, de incentivo no aperfeiçoamento do sistema de controlo interno e de inferência na segurança nas recomendações prestadas às administrações das organizações.

Consequentemente, a Auditoria Interna (AI) que tem vindo ao longo dos anos a desenvolver-se a par com as necessidades das organizações e a adquirir especial interesse pelas mesmas, no sentido em que apoia a totalidade dos controlos intrínsecos a todos os departamentos existentes numa Organização.

### 2.2.1 Conceito e Evolução Histórica

A AI tem vindo a categorizar-se como uma base imprescindível para as organizações, no apoio à gestão e no alcance dos objetivos, proporcionando que retirem o melhor proveito dos seus recursos, minimizando os custos e os riscos intrínsecos às áreas de negócio, fomentando com isso maiores incrementos ao nível da rentabilidade.

Em meados do Séc. XVIII com a revolução industrial e posteriormente com a crise financeira deu-se a eclosão da AI em corolário da necessidade de resposta às organizações, na procura de prova e de garantir um maior controlo nas transações financeiras. Na época, os colaboradores afetos às organizações tornaram-se imprescindíveis na procura e recolha dos documentos, por forma a auxiliar os auditores externos e conjuntamente reduzir custos, mas também aperfeiçoar o controlo das contas das organizações.

Com a expansão dos mercados e a propensão dos processos produtivos, as organizações chegaram à conclusão de que as auditorias anuais, efetuadas pela auditoria externa, eram diminutas dando lugar de atuação à auditoria interna.

Novas regras foram instituídas no seio dos profissionais de auditoria definindo, segundo Moeller (2009, p.5), que as auditorias deviam ser concretizadas com base numa «[…] *limited sample of transactions, along with greater reliance on internal control procedures»* onde o trabalho efetuado pelos profissionais centralizava-se na confirmação dos *«[…] accounting records and detecting financial errors and irregularities*».

Em analogia, Costa (2017, p.117) defende que o trabalho do auditor interno estava inicialmente focado para a área financeira com funções como a «[…] salvaguarda dos ativos [..], a verificação do cumprimento dos procedimentos estabelecidos pelo órgão de gestão e a constatação acerca da credibilidade da informação financeira».

Em 1941 é fundado o IIA - The Institute of Internal Auditors como «[…] i*nternal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator*.» e em 1978 define o conceito de AI como sendo:

> […] *an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes*».

Em 1992 foi criado o Instituto Português de Auditores Internos (IPAI) que representa o IIA em Portugal. Mais tarde, em 2002, em detrimento de uma crise financeira foi redigida uma lei, que veio evidenciar a importância da AI para as organizações, com o propósito de «[…] proteger os investidores melhorando a precisão e a fiabilidade das demonstrações financeiras» das empresas. (Costa, 2017, p.69).

Poder-se-á considerar a atividade de AI como autónoma e de consultoria, em permanente desenvolvimento, de apreciação objetiva, designada a acrescentar valor e a aperfeiçoar as operações de uma Organização. Para Martins e Morais (2013, p.91):

> «[a] auditoria é uma função contínua, completa e independente, desenvolvida na entidade, por pessoal desta ou não, baseada na avaliação do risco, que verifica a existência, o cumprimento, a eficácia e a otimização dos controlos internos e dos processos de *Governance*, ajudando-a no cumprimento dos seus objetivos».

Partindo de semelhante ponto de vista, Pinheiro (2014, p.33) defende que o principal intuito da AI, passa por «auxiliar a empresa e todos os níveis de gestão no cumprimento das suas responsabilidades em promover sistemas de controlo adequados, visando a melhoria da performance e do desenvolvimento sustentável da empresa».

Com o propósito de alcançar o melhor partido dos recursos existentes, a AI primazia a redução dos custos e mitiga os riscos intrínsecos às áreas de negócio, com o intuito de maximizar o desenvolvimento e os proveitos de determinada organização. Taborda (2015, p.15) caracteriza esta atividade «[…] como uma técnica de controlo de gestão que incide na análise, verificação e avaliação das atividades da entidade e da eficácia e conformidade do funcionamento de outras técnicas de controlo».

Possui a missão de analisar e aquilatar os métodos e comportamentos das organizações, para que possa apoiar os restantes membros, na persecução plena das suas funções.

Na opinião de Teixeira (2006, p.32) «[…] a AI deve ser vista como uma atividade que pretende acrescentar valor à Organização, contribuindo para a satisfação dos seus objetivos» para tal o auditor interno tem de assegurar uma boa relação com a Organização e «com todos os restantes serviços, sendo para tal necessário que exista um conhecimento generalizado sobre a sua existência, suas funções, objetivos e meios».

A função da AI pode ser desempenhada por elementos que pertencem à própria Organização e que fornecem à mesma, relatórios com avaliações, estudos, melhorias, recomendações, bem como, outras informações que sejam pertinentes em qualquer atividade auditada, incluindo a promoção de controlos mais eficazes a custos razoáveis.

De acordo com Taborda (2015, p.15) «[c]onsiste num serviço criado pela (e para a) própria entidade, contribuindo para o auxílio do órgão de gestão no cumprimento dos objetivos organizacionais». Auxilia e acompanha a organização na concretização dos seus objetivos, através de uma abordagem metódica e sistemática, para avaliar e melhorar a efetividade dos métodos de controlo de riscos e gestão.

Para tal estabelece objetivos estratégicos, procedimentos e planos de ação, de modo a sistematizar os resultados observados podendo recomendar à administração correções com o intuito de melhorar a atividade da empresa.

Sucintamente, poder-se-á concluir, que a atividade de AI é uma ferramenta indispensável para o órgão de gestão, visto que apoia através da mensuração e avaliação da eficiência e eficácia dos principais departamentos existentes na Organização, utilizando as diretrizes, políticas e objetivos que foram antecipadamente determinados pela administração.

Tudo isto com o propósito de proporcionar à Organização, uma maior confiança e segurança na execução das suas funções. Conforme Rubio, Silva e Guimarães, (2014, p.6) estabeleceram «[…] a função da auditoria interna é contínua, ela atua na Organização para garantir e preservar a 'saúde' da mesma, pois somente através de exames periódicos e sucessivos é que poderá apresentar um parecer/relatório confiável, seguro, completo».

### 2.2.2 O Papel e as Funções da Auditoria Interna

O célere desenvolvimento do mercado empresarial, quer em termos dimensionais, tecnológicos ou até mesmo na amplitude das áreas de negócio inerentes, resulta cada vez mais numa complexa e exigente monitorização dos procedimentos de uma Organização.

Os auditores internos passaram, no âmbito das suas funções, do apoio à área financeira e contabilística para ocupar cargos de controlo administrativo, com o propósito de aquilatar a eficácia dos processos operacionais e a efetiva utilização dos controlos internos nas diversas áreas de empresa, desempenhando funções, de elevada importância, ao nível da assessoria e do apoio à gestão na implementação de melhores mecanismos de controlo interno. Pinheiro (2014, p.35) refere o trabalho realizado pelo auditor interno como:

> "[…] deverá ter como objetivo fundamental apresentar os resultados dos trabalhos realizados com a oportunidade necessária, de modo que as propostas de recomendações possam ser implementadas adequadamente e contribuir, objetivamente, para a melhoria do desempenho de toda a empresa, numa lógica de satisfação dos clientes.

São frequentemente colaboradores da empresa que têm como função, reconhecer as fraquezas da empresa ao nível do sistema de controlo interno, estabelecer os factos que originaram a ocorrência de fraude e ter perceção dos seus efeitos de modo a implementar medidas corretivas.

Pode-se considerar como um «[…] *front-line set of eyes and ears for the audit committee and senior management*» (Moeller, 2009, p.153).

Na opinião de Morais & Martins (2013, p.92), o auditor interno executa a sua avaliação, mediante uma criteriosa análise, que tem por base a identificação e apreciação dos riscos, a «[…] razoabilidade, a suficiência e aplicação dos controlos contabilísticos, financeiros, operacionais, processos e de gestão» e assegura o cumprimento, melhoria e a adequação dos processos «[…] dos controlos internos» e «[…] de *Governance*».

Visa ainda, para além de apoiar o órgão de gestão na tomada de decisão, assegurar as políticas e procedimentos instituídos de forma a serem observados dentro da Organização contribuindo para a melhoria do desempenho da entidade, mediante avaliações às ineficiências do sistema de controlo interno. Executa avaliações periodicamente, incluindo igualmente outras áreas que não apenas as associadas à gestão, como é o caso do sistema de controlo de qualidade ou a gestão dos recursos humanos.

Com base nas suas avaliações, elaboram relatórios com recomendações que possibilitem ao órgão de gestão, definir métodos prudentes, capazes de ultrapassar as barreiras existentes, permitindo uma melhoria da eficiência e eficácia organizacional. Os relatórios de AI destinam-se à administração da empresa e recaem sobre todas as funções económicas da Organização.

No âmbito das funções do auditor interno, faz parte a cooperação com a auditoria externa através da partilha de registos, da investigação da observância dos regulamentos e procedimentos internos, colaboram com os gestores operacionais no reconhecimento das condutas internas para uma melhoria do desempenho, intercedendo ao nível das áreas que carecem de maior atenção e consequentemente que necessitam de reduzir riscos.

Aperfeiçoam os índices de rentabilidade e a capacidade de resposta, contribuindo para que os objetivos da empresa possam ser atingidos do modo mais eficaz possível. Barreiro (2007, p.27), refere que o auditor interno é uma mais-valia para a Organização na medida em que «[…] um departamento de AI, competente e atuante, pode, atempadamente, evitar a eclosão de fraudes ou de outro tipo de comportamentos lesivos quer morais quer materiais, antiéticos ou, simplesmente, de natureza desviante.».

Apesar de a deteção da fraude não ser o principal objetivo/propósito, este deve ter também um papel fulcral no exercício das suas funções, assim como, possuir conhecimento suficiente acerca do tema da fraude, para que consiga reconhecer e diferenciar os numerosos indicadores existentes, os tipos de fraude, as características decorrentes de um acontecimento de fraude e as técnicas que deverão ser utilizadas.

Nas circunstâncias em que detete uma situação irregular, deve ponderar e avaliar se existe ou não a necessidade de em primeira instância, investigar o evento e posteriormente notificar as autoridades competentes. É de igual forma expectável que, perante a perceção da existência de debilidades no controlo interno permanecer alerta, pois poderá ser um indício da existência da ocorrência de fraude.

Para corresponder ao principal objetivo da AI, os auditores devem fazer um levantamento contínuo aos procedimentos, determinar a sua tipicidade e avaliar se a informação recolhida corresponde aos critérios estabelecidos. Na opinião de Lajoso (2005, p.11), deve ser fornecido à Organização, análises que digam respeito à «[…] eficiência e eficácia das operações, incluindo os controlos não financeiros de uma entidade; a revisão do cumprimento das leis, regulamentos e outros normativos externos com as políticas e diretivas da administração e outros requisitos internos».

São, por estes motivos, cada vez mais nomeados para ajudar as empresas, de forma a mitigar os riscos inerentes ao negócio, colocando esses riscos em níveis aceitáveis para a Organização, simplificando tarefas e reduzindo custos, avaliando e monitorizando as operações, de forma pormenorizada e exaustiva.

Concluídas as análises e as respetivas avaliações, o auditor deve fornecer ao órgão de gestão recomendações permitindo à Organização incrementar os índices de rentabilidade e atingir um controlo mais eficaz das operações.

## 2.3 Auditoria aos Sistemas de Informação

Em virtude de um mundo globalizado perante uma sociedade contemporânea, composta por empresas de elevada dimensão e com o crescente progresso económico e tecnológico dos países evoluiu-se para uma gradual complexidade ao nível da gestão dos negócios, onde as operações são registadas em tempo real, razão pela qual o conceito de Auditoria a Sistemas de Informação (ASI) se tenha dispersado e desmistificado ao longo do tempo.

Atualmente, com a constante implementação de procedimentos tecnológicos nos SI das organizações, aumenta o número de riscos intrínsecos aos SI que necessitam de ser orientados, controlados e mitigados.

Buckinham, Hirschheim, Land & Tully (1987 citado por Avison e Myers[4], 1995, p. 75) definem o conceito de SI como «[…] *a system which assembles, stores, processes, and delivers information relevant to an organisation (or to society), in such a way that the information is accessible and useful to those who wish to use it.*»

A função da ASI revela-se diariamente mais preponderante para aferir a robustez dos sistemas de controlo interno das organizações e concludentemente sobre os impactos que tem nas atividades das empresas e dos seus relatórios financeiros.

Veio a desenvolver, à medida do tempo, o seu campo de atuação por forma a não só reconhecer e examinar as fontes e os SI como também, assegurar uma avaliação criteriosa aos métodos adotados na utilização destes sistemas, à respetiva ligação destes com as áreas de negócio e com os objetivos da empresa.

De acordo com Weber (1999 citado por Oliveira[5], 2006) a ASI consiste num:

> "[…] processo de recolha e avaliação de evidencias para determinar se um sistema computadorizado salvaguarda os bens, mantém a integridade dos dados, permite atingir os objetivos da Organização de forma eficaz e utiliza os recursos de forma eficiente".

Segundo Soares (2010) é uma «[…] atividade de recolha e avaliação de evidências com vista a determinar se um sistema de informação goza de integridade, se contribui para o alcance eficaz dos objetivos organizacionais».

Complementarmente, qualifica a ASI como uma atividade imprescindível a qualquer Organização na medida em que «[…] utiliza os recursos que lhe estão afetos de forma eficiente» e assegura que a Organização «[…] dispõe das competências, processos e recursos necessários e suficientes para o cumprimento da sua missão.».

4 Buckingham, R. A., Hirschheim, R. A., Land, F. F., & Tully, C. J. (Eds). (1987). *Information systems education: Recommendations and implementation*. Cambridge: Cambridge University Press

5 Oliveira, J. A. (2006). Método de Auditoria a Sistemas de Informação. Porto: Porto Editora.

Na opinião de Carneiro (2004, p.19) a noção de ASI consiste «[…] na análise e avaliação, quer envolvendo-se em processos de planeamento, desenvolvimento, testes e aplicação de sistemas, quer examinando a estrutura lógica, física, ambiental, organizacional de controlo, segurança e proteção de dados.». O autor defende ainda que o propósito da ASI não é meramente informático, mas sim «[…] focalizando-se em todos os SI, informatizados ou não, que existem na Organização».

Segundo Oliveira (2006, p.75) a ASI define-se como:

> «[…] a revisão dos sistemas de informação, para verificar se realizam as funções e operações para as quais foram criados, assim como comprovar se os dados e demais informações neles contidos correspondem aos princípios de fiabilidade, integridade, precisão e disponibilidade».

O foco principal da ASI deixou de ser a informação, no sentido restrito da palavra, para passar a ser o ponto de relação entre as necessidades das organizações com os SI que estas possuem, nomeadamente, no que concerne às normas e procedimentos certificar o cumprimento e a conformidade face à legislação vigente, assegurar que exista validações à natureza, capacidade e aplicabilidade dos sistemas implementados e apreciação do âmbito de atuação do SI perante circunstâncias de rotura.

## 2.4 O Alojamento Local

Perante uma profunda globalização e evolução tecnológica, na segunda metade do Séc. XX, as distâncias entre os países diminuíram, houve um reforço dos mercados tradicionais e a emergência de novos o que, em simultâneo com o desenvolvimento da *Internet*, proporcionou um aumento considerável do turismo em todo o mundo e concludentemente, na variação da oferta turística.

O AL tem vindo, ao longo do tempo, a ser entendido como uma prestação de serviços de interesse de ordem pública, económica, social e cultural a nível global.

O acelerado crescimento do turismo deixou Portugal na 12.ª posição no ranking mundial da competitividade de destinos turísticos de acordo com o relatório "*The Travel & Tourism Competitiveness Index 2019*" do *World Economic Forum.*

### 2.4.1 Conceito e Evolução Legislativa

Surpreendentemente, o AL não é uma temática recente embora se tenha fundido por todo o mundo com a evolução da economia digital e do comercio eletrónico. Desmistificando, é possível dizer que o AL é precedente a outros conceitos associados à área de negócio do turismo, de habitação de curta duração, na época as denominadas estalagens ou albergues que vieram ao longo do tempo a difundir-se por toda Europa.

Num período em que o turismo, no mundo e em Portugal, ainda era embrionário surge o contrato de albergue como a primeira menção legal de alojamento. A nível nacional, consta do Código Civil de Seabra, de 1867, no seu artigo 1419.º, tipificado o contrato de albergaria e caracterizado como «[…] quando alguém presta a outrem albergue e alimento, ou só albergue, mediante a retribuição ajustada ou de costume».

Estas estalagens ou albergues à semelhança do AL baseavam-se na hospedagem em moldes de habitação de utilização corrente e de reduzida duração, enraizada no comércio local, prestando um serviço familiar. Posteriormente em 1921, com a Lei n.º 1152, foi através do seu artigo 5.º que surgiram as primeiras taxas de turismo afetas às organizações públicas de turismo local, as intituladas comissões de iniciativa.

Os consumidores que se hospedassem em albergues nas estâncias climáticas, de altitude, repouso, recreio e turismo ou que alugassem habitação ficariam sujeitos a uma taxa turística. É em 1957 que surge, a primeira lei das regiões de turismo, o Decreto n.º 41035, para dar resposta ao fluxo de turistas a nível regional, onde no seu artigo 5.º, n.º 4, previa registar e manter atualizado a inscrição dos alojamentos, ou áreas destes, destinados ao arrendamento e sublocação, localizados nos centros turísticos, procedimentos que foram revogados em 1997, através do Decreto-Lei 167/97.

No entanto, foi em 1954 com a Lei nº 2073 que se viu estabelecido na alínea a) do artigo 1.º os conceitos elementares de estabelecimento hoteleiro existentes até então, detalhadamente estavam incluídos os hotéis, pensões e hospedarias, as pousadas e estalagens. Ainda assim, existia uma lacuna na legislação uma vez que não englobava as diferentes tipologias de alojamento do foro privado e que segundo Brito (2010, p.54) «[a] lei de 1954 não prevê o futuro.».

Mais tarde, a 25 de novembro de 1966 é aprovado pelo Código Civil Português, artigo n.º 1083, o conceito de alojamento temporário que deixa de ser regulado como um contrato e passa a ser ajustado com uma operação económica autonomizada de atividade turística.

E em 1886 é estatuído o conceito de alojamento privado, ao abrigo do Decreto-Lei nº 238/86, onde «Para além dos empreendimentos referidos […], poderão ainda ser declarados de interesse para o turismo os alojamentos particulares». Não obstante, apenas os alojamentos que se encontrassem registados de acordo com as normas estatuídas pelo Decreto-Lei nº 14/78 poderiam ser comercializados.

O aparecimento das novas comunicações aéreas no início do Séc. XXI, no âmbito do turismo, beneficiou a Europa com novas rotas e uma maior facilidade de mobilização entre fronteiras, provenientes de companhias de aviação de baixo custo, que dera origem a uma enorme reforma ao nível da rede de transportes, de serviços culturais e turísticos, permitindo a requalificação e reabilitação urbana dos seus centros históricos.

De acordo com Seixas (2019, p.9), no plano do AL «O processo de massificação ganhou forma a partir do final do Séc. XIX, como consequência da industrialização, da melhoria dos transportes e do acesso de um maio número de pessoas ao tempo livre.».

Com a reabilitação urbana e com o aumento gradual do turismo surge uma panóplia de conceitos de alojamentos turísticos existentes no país que tornou imperativo uniformizar num só documento toda a regulamentação afeta a alojamento turístico.

Brauckmann (2017) defende que o desenvolvimento deste setor está fortemente sustentado por dois motivos «*The first of these is the increasing appeal of cities and city tourism; the second is the new, internet-based booking platforms that facilitate the spread of alternative accommodation offerings*.».

Surge neste contexto, em Portugal, resultante do Decreto-Lei n.º 39/2008, de 7 de março, a figura jurídica de AL, por forma a regulamentar as prestações de serviços de alojamento temporário, em habitações que não cumpram com os requisitos necessários para serem considerados empreendimentos turísticos.

É em virtude da alínea b) do artigo 2.º que não são considerados empreendimentos turísticos «As instalações ou os estabelecimentos que, embora destinados a proporcionar alojamento temporário com fins lucrativos, revistam natureza de alojamento local nos termos do artigo seguinte.», ou seja, por empreendimentos turísticos compreende-se os hotéis, apart-hotéis e pousadas que possuam características específicas, os aldeamentos e apartamentos turísticos, os resorts, os parques de campismo e caravanismo.

Naturalmente, surge espelhada no artigo 3.º do mesmo decreto, a categorização de alojamento local como estabelecimento que deve constar nos registos das câmaras municipais sob a modalidade de moradias como edifício autónomo ou unifamiliar, apartamento como fração independente de um edifício, estabelecimentos de hospedagem constituídas por quartos ou os designados *hostels*[6].

Caracteriza-se por ser um modo de alojamento familiar, sob dessemelhantes tipologias, na medida em que, se disponibilizam habitações tradicionais, podendo existir inclusive situações em que as habitações são partilhadas e são disponibilizadas áreas específicas, como quartos e áreas comuns. Cumpre ainda, conforme no n.º 2 do artigo 43.º do DL 39/2008, mediante certificação de uso, fornecer, através de um imóvel mobilado e equipado, serviços de alojamento turístico ao público em geral, por períodos inferiores a 30 dias, onde estão incluídos serviços de estadia, limpeza e receção.

Mais tarde com a Portaria 138/2012, foi criado o Balcão Único Eletrónico, uma plataforma informática nacional que consente, de modo gratuito, mediante comunicação prévia ao presidente da Câmara Municipal (CM), territorialmente competente, o registo dos estabelecimentos de exploração de AL, que em Portugal são obrigatórios.

Atualmente, para a exploração dos estabelecimentos de AL, vigora a Lei n.º 62/2018, de 22 de agosto de 2018, resultante da revogação do Decreto-Lei n.º 128/2014, que já havia sido alterado através do Decreto-Lei n.º 63/2015. Para regulamentar esta nova realidade, foi modificado o conceito de estabelecimento de AL, colocando de lado a restrição à exploração através do pressuposto da existência de turistas como elemento crucial para a exploração desta atividade, assim, a atividade de AL deixou de estar restrita à qualidade dos hospedados, sendo o conceito de turistas unicamente ilustrativo.

Na realidade, a legislação veio tornar esta noção mais inclusiva, no sentido em que inclui qualquer estabelecimento que preste, mediante remuneração, serviços de alojamento de curta duração. Esta lei veio acrescentar às modalidades já existentes os "quartos", conforme demonstrado na Figura 2.1, que veio abranger os casos em que a exploração de AL é feita no domicílio fiscal do locador, sendo a unidade de alojamento o quarto, esta situação só é possível até perfazer o número máximo de três quartos da sua residência.

[6] *Hostels* são estabelecimentos destinados à hospedagem turística, cuja unidade de alojamento predominante é o dormitório.

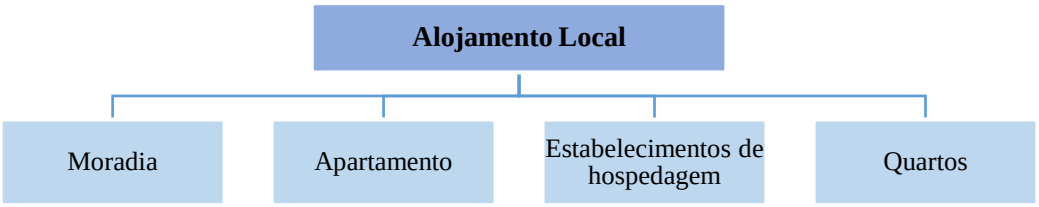



**Figura 2.1 -** Modalidades do Alojamento Local

Uma outra modificação igualmente relevante, introduzida pela Lei 62/2018, prende-se com a salvaguarda dos condomínios, perante os estabelecimentos de hospedagem que se qualifiquem como *hostel*, sob a forma de prédio em propriedade horizontal. Nestas circunstâncias e quando nos mesmos se verifiquem estar afetas frações destinadas à habitação, a acomodação e exploração carece da autorização do condomínio, sob a forma de ata de assembleia, que deverá ser entregue conjuntamente com a comunicação à CM.

Segundo o artigo 4.º, 6.º e 9.º da referida Lei, esta permite, por meio de deliberação em assembleia de condóminos, contestar o pleno exercício de funções destes estabelecimentos, ainda que a comunicação prévia tenha sido corretamente feita, o condomínio pode pedir a anulação do registo do *hostel*.

Também o presidente da CM pode determinar o cancelamento do registo perante situações em que exista divergência com a informação ou documentação inerente à realização do registo, incumprimento dos requisitos aplicáveis aos estabelecimentos, sejam instalados novos alojamentos em infração de áreas de contenção. Que isto dizer que, pode impor limite ao número de AL em determinada freguesia ou nos casos em que o proprietário de exploração não cumpriu com a obrigatoriedade de celebrar contrato ou manter válido o seguro de responsabilidade civil.

Segundo Gutiérrez, J., García-Palomares, J. C., Romanillos, G., & Salas-Olmedo, M. H. (2017) «*Over the last few decades urban tourism has undergone huge growth and has become an extremely important activity in many cities, which have seen themselves inundated by crowds of tourists pursuing diverse activities.*».

Portugal não é exceção e o vasto número de entradas diárias de turistas em território nacional justificou a necessidade de uma nova regulamentação que surgiu, recentemente, a 6 de novembro de 2020, a Portaria n.º 262/2020.

Esta visa condições de funcionamento, incumbe a obrigatoriedade da identificação dos estabelecimentos de AL em atividade e apresenta novidades como o reporte das dormidas e medidas de sustentabilidade ambiental. Neste sentido, os estabelecimentos de AL ficam sujeitos, com período transitório de 12 meses, a contar da data da portaria, a adotar as condições mínimas de funcionamento impostas.

Embora muitas destas condições já estejam implementadas pelo setor do AL, outras vêm introduzir inovação à prestação de serviço deste setor, incluindo um conjunto de condições de sustentabilidade, por forma a dar resposta às políticas de sustentabilidade da Estratégia Turismo 2027.

Nomeadamente, a aplicação de procedimentos que intentem para o consumo eficiente de água e energia, a disponibilização e utilização de produtos de limpeza e higiene biodegradáveis, assim como, de reciclagem para a separação de resíduos sólidos urbanos.

São de igual modo condições de sustentabilidade a utilização de equipamentos com eficiência energética elevada, a disponibilização de formação permanente aos seus colaboradores de boas condutas ambientais de trabalho e obter certificados ambientais ou selos de qualidade ambiental atribuídos por entidades nacionais ou internacionais competentes. Na Figura 2.2 estão representadas algumas das funcionalidades comuns impostas pela Portaria n.º 262/2020, a estes estabelecimentos de turismo.


**Figura 2.2 -** Condições de funcionamento no Alojamento Local

De facto, o AL veio instituir, face aos empreendimentos turísticos tradicionais, uma alternativa na qual os legisladores procuraram enquadrar, ao longo dos tempos, um conjunto de realidades intrínsecas à prestação de serviços de alojamento turístico, sem que houvesse legislação devidamente articulada.

Esta atividade não só veio inovar a tradicional indústria hoteleira como apresenta valores consideravelmente baixos, comparativamente com os típicos hotéis, tornando-se um negócio extremamente atrativo, rápido e fácil para o consumidor, mas também extremamente rentável ao Estado e por isso necessário de legislar.

O AL resulta do arrendamento temporário de habitações para fins turísticos, sobretudo, através das plataformas online que publicitam as instalações das habitações e disponibilizam informações como a localização, as comodidades, os contactos e os métodos de pagamento. É de referir que todo o processo, desde o momento da reserva e à finalização da compra e que é espelhado por plataformas digitais, foi idealizado e pormenorizado para que a experiência do consumidor possa ser o mais intuitivo e rápido possível, conforme representado na Figura 2.3.

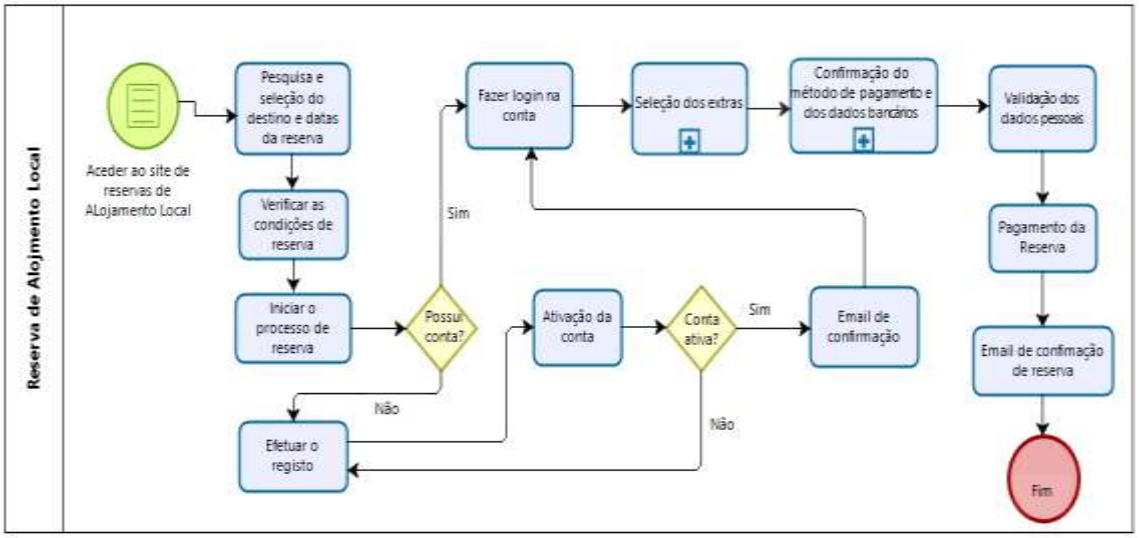



**Figura 2.3 –** Notação BPMN da reserva / compra de AL online

Tome-se como exemplo, representado pela Figura 2.3., o caso de plataformas como a *Homeaway*, *Booking* ou *Airbnb* que são exemplos de plataformas *online*, que resultaram desta conjuntura de crescimento e diversificação, facto que, nos últimos anos, veio aumentar expressivamente a recapacitação e o proveito de imóveis para alojamento temporário a turistas exteriores ao circuito tradicional da hotelaria.

### 2.4.2 Os Impactos Atuais no Alojamento Local

Num tempo marcado por uma globalização contínua, da produção e do consumo de produtos e serviços, intensificada através dos novos acordos de mercado e pela remoção das barreiras às transações internacionais deu-se um aumento significativo da procura do turismo e naturalmente do AL.

Por efeito, o desenvolvimento da economia digital, das redes de transportes e dos novos serviços culturais e gastronómicos, implementados por todo o mundo, contribuíram substancialmente para a materialização da oportunidade de requalificar e reabilitar as zonas urbana dos centros históricos, permitindo que o AL se desenvolvesse.

O impacto exponencial do AL resulta, em grande parte, do crescimento colossal do setor do turismo e do comércio digital que sustentam esta área de negócio, tendo sido por isso, pela dimensão que possui na sociedade, pelas receitas que disponibiliza e pelo tanto que contribui para a saúde da economia, imperativo a instituição de um regime legal próprio.

O célere crescimento das novas tecnologias, associadas a plataformas turísticas, tem vindo não só a valorizar novos modelos de negócio como também novas tipologias de alojamento. De acordo com o artigo de Munkøe (2017), "*Regulating the European Sharing Economy: State of Play and Challenges*" nos últimos anos,

> «[…] *the sharing economy has gone from niche to mainstream. From its humble beginnings as Air Bed and Breakfast, which hosted conference attendees on airbeds in the home of its founders, Airbnb has become a global entity with a market capitalization that exceeds those of "traditional" major hotel chains* […]».

Conforme mencionado no relatório da EY & AM&A (2017), "O avanço da economia digital a nível nacional", resulta da «[…] presença constante da internet na rotina diária das populações, o uso de produtos digitais está a tornar-se uma alternativa válida aos produtos físicos em geral.», consentindo que estes consumos se revelem «extremamente acessíveis a qualquer momento e em qualquer lugar, são uma boa ferramenta para economizar tempo e espaço.».

Com o progresso da economia digital revelou-se notória a importância da *Internet* como meio de comunicação, informação e comercialização, permitindo diversificar a oferta de serviços associados ao AL, reduzir os seus custos e obter um alcance global que permitiu influenciar as escolhas dos consumidores.

Na opinião de Zeferino (2016, p.22) a transformação digital das empresas:

> «[…] vai muito mais longe no seu papel reformista, porque implica o uso de metodologias que visem claramente encontrar benefícios em toda a estrutura da Organização, nomeadamente, ganhos de eficiência, melhoria efetiva de processos e criação de uma identidade e cultura baseadas nesta atitude.»

O AL veio, através da economia digital, disponibilizar um serviço familiar, com custos reduzidos, face aos praticados pela hotelaria tradicional, através de formatos menos convencionais, criando proximidade com os consumidores. Segundo Munkøe (2017) grande parte do sucesso do AL deve-se ao facto de «[…] *transaction costs have been massively reduced, since internet technology allows information to be exchanged virtually instantly at no cost.*».

Desta forma, permite que o setor alcance um variado leque de consumidores, que não se identificam com a indústria hoteleira, quer seja por razões económicas ou simplesmente porque o alojamento confere a privacidade e a singularidade que muitos procuram.

Segundo Zeferino (2016, p.22 - 23), «[…] a economia e a sociedade digital englobam todas as atividades naquelas áreas que possam ser potenciadas por via das tecnologias digitais, em que o exemplo mais concreto é o comércio eletrónico.».

O comércio eletrónico surgiu em meados dos anos 90 e está associado à utilização de instrumentos eletrónicos ou da *Internet*, sejam eles o computador, telemóvel, e-mail ou outro aparelho eletrónico para adquirir bens e/ou serviços.

A facilidade de acesso e o alto grau de dispersão, inerentes ao comércio eletrónico, foram fatores decisivos que contribuíram para que as empresas de AL usufruíssem de plataformas digitais onde podiam exibir os serviços que comercializavam, de modo acessível, em qualquer parte do mundo e a qualquer hora do dia, o que até então não era possível e estariam condicionados aos clientes locais.

O desenvolvimento do comércio eletrónico, trouxe um maior número de oportunidades face às limitações que encontrariam nos mercados locais, como é o caso da dispersão geográfica, da facilidade de acesso e da proximidade com o cliente ainda que este habite em outra cidade, em outro país ou continente.

A oferta constante e imediata de informação a nível global, a criação de novos meios de comunicação e de sistemas de reservas/pagamento, a gradual automatização das transações e dos procedimentos inerentes à gestão e ao consumo, são alguns dos pontos que beneficiam a atividade do AL.

Acresce também a acentuada predominância do marketing digital, o evidente interesse da população com a conectividade e com as redes digitais e a gradual democratização do interesse pela cultura fundamentada pela partilha e pelo acesso ao conteúdo online.

A procura prévia por informação respeitante a serviços, viagens, alojamentos, acrescenta conhecimento prévio ao consumidor e naturalmente, aumenta as expectativas sobre esses serviços e destinos, bem como, pela procura de ofertas únicas e interativas.

Segundo Garcia (2017)

> «[…] no passado os arrendamentos particulares a turistas tinham por objeto, sobretudo, imóveis localizados perto de praias ou termas e ocorriam nos meses de Verão, atualmente os turistas procuram imóveis localizados nos centros históricos das grandes cidades e durante todo o ano.»

Através do comércio eletrónico, os consumidores de AL optam por novas experiências e conseguem usufruir das suas estadias de forma facilitada e harmoniosa, muito pelo facto das plataformas digitais, permitirem comparar, com maior facilidade, os preços face aos serviços oferecidos e consultar informação turística e cultural, em tempo real, desde verificar preços e horários de determinado ponto turístico a pesquisar quais os restaurantes mais conceituados face à localização onde se encontram.

É possível identificar ao nível estratégico através de uma análise de diagnóstico realizada, os pontos críticos inerentes à atividade de AL. A análise SWOT realizada, teve por base os contextos económicos, ambientais, tecnológicos, demográficos, socioculturais e a mobilidade, na ótica das empresas, conforme apresentado na Figura 2.4.

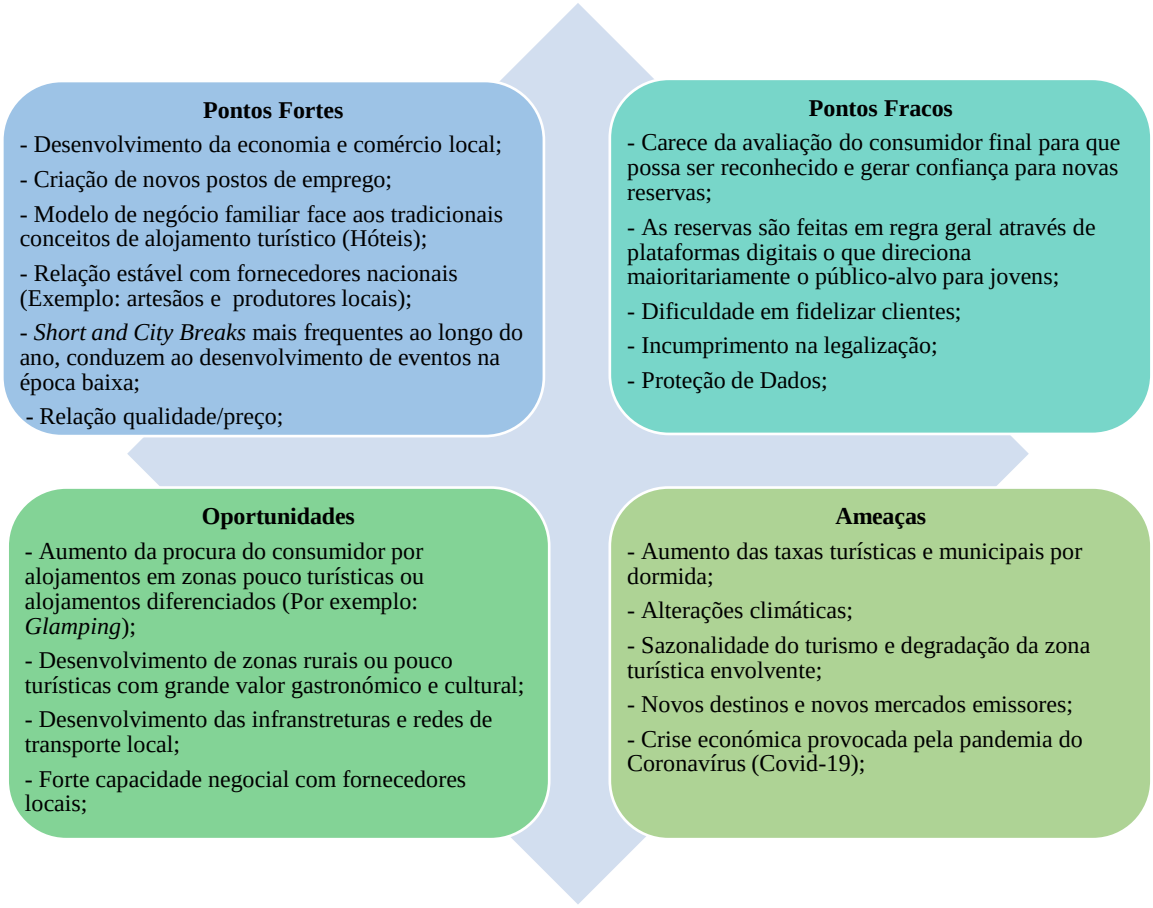



**Figura 2.4 -** Análise SWOT na ótica das organizações de AL

Parte dos impactos demográficos e socioculturais do AL passam pelo envelhecimento populacional que não tem tanta interação com as plataformas digitais e por isso não recorre tantas vezes a este tipo de serviço.

Com igual peso, também a preocupação crescente com a alimentação, o bem-estar e o ambiente, a constante alteração das necessidades/preferências, a procura por alojamentos únicos e diferenciados faz com que, cada vez mais, tenha de existir um maior investimento por parte destas empresas para dar resposta às necessidades dos consumidores e ir ao encontro dos ideais destes.

Atualmente, as questões ambientais são uma constante preocupação para estas empresas, para além dos casos mais comuns, como é o caso, da erosão costeira nos alojamentos que se encontrem em destinos de sol e praia existe também um cuidado redobrado com a adoção de comportamentos sustentáveis, o ruído e poluição.

Segundo o artigo "When Tourists Move In: How Should Urban Planners Respond to Airbnb?" Gurran, N., & Phibbs, P. (2017) AL «[…] *has expanded globally, raising substantial planning and regulatory concerns. We ask whether rentals generate significant neighbourhood impacts like noise, congestion, and competition for parking*».

Muito valorizado pelos hóspedes, são exemplos de comportamentos sustentáveis os alojamentos possuírem espaço reservados para a reciclagem, tomadas inteligentes que reduzam o consumo de energia ou disponibilizarem shampoo ou gel de banho sólidos minimizando o consumo de plástico.

Por outro lado, o ambiente global é cada vez mais competitivo e os hóspedes estão cada vez mais atentos à relação qualidade-preço, assim como, a novos destinos e a novos mercados emissores. De acordo com Garcia (2017) «[…] registam-se também mudanças geográficas e um certo esbatimento da marca de sazonalidade que os fluxos turísticos anteriormente apresentavam.».

Ainda assim, a emergência de novos mercados, contribui para as economias em transição, como é o caso da Ásia e o crescimento do rendimento *per capita* nos países mais desenvolvidos torna-se favorável para o AL, no que respeita à economia.

Na opinião de Garcia (2017)

> «[…] no passado os arrendamentos particulares a turistas tinham por objeto, sobretudo, imóveis localizados perto de praias ou termas e ocorriam nos meses de Verão, atualmente os turistas procuram imóveis localizados nos centros históricos das grandes cidades e durante todo o ano.»

O aumento da globalização é proporcional às expectativas dos consumidores, quer isto dizer que, impõe que exista uma maior divulgação de informação através das plataformas digitais dos serviços que os alojamentos dispõem e do meio envolvente onde estão inseridos. Acresce ainda a dificuldade de fidelizar os hóspedes, uma vez que, existe a tendência de não repetir o mesmo destino e a procura por novos destinos/experiências.

Importa salientar a importância da mobilidade, quer isto dizer que, a presença de companhias aéreas de baixo custo e de aeroportos secundários, assim como, a existência de linhas férreas que incluam comboios de alta velocidade, uma boa rede de transportes ou terminais de cruzeiro, com preços reduzidos e boa qualidade de serviço, são fatores decisivos no momento de escolhas dos consumidores.

Os transportes são um ponto essencial para o sucesso das empresas de AL, uma vez que, quando optem por imóveis que não se encontram centralizados nas zonas turísticas, estes devem estar fortemente sustentados por redes de transportes que permitam aos consumidores rapidamente deslocarem-se até aos centros das cidades.

Razão pela qual na Europa tem sido feito de modo crescente, um reordenamento turístico aos centros urbanos com alargamento das delimitações de circulação dos meios de transporte, potenciado a criação de plataformas intermodais.

Não só as empresas de AL beneficiaram do comércio eletrónico, o consumidor também privilegiou, por exemplo, no facto de não ter de se dirigir a um espaço físico como é o caso das agências de viagens para adquirir determinado serviço. Conseguiu obter, através de plataformas digitais, como é o caso do *Airbnb* ou *Homeaway*, uma maior diversidade de serviços, uma vasta abundância de preços e por sua vez, uma facilidade imediata na comparação da relação preço/qualidade.

Com o aumento da procura e da competitividade de preço também a publicidade de alojamentos não legalizados e de falsos alojamentos aumenta assim como acomodações que não reúnem os requisitos de saúde pública, roubos de identidade, dados bancários entre outros. De acordo com o artigo "Global Home-Sharing, Local Communities and the Airbnb Debate" de Gurran, N (2017) «*A primary risk arising from online accommodation platforms is that they enable unlicensed accommodation providers who do not comply with the existing public health and safety*.».

Face ao apresentado, revela-se pertinente analisar se perante a extensão e relevância económica, o AL não carece de uma legislação jurídica e/ou regulatória complementar específica, por forma a dar resposta aos interesses económicos do Estado e aos direitos de proteção de dados e de privacidade dos consumidores.

O AL necessita dos dados pessoais que recolhe para valorizar os seus serviços, acrescentando valor às experiências que vai disponibilizar aos seus clientes e à própria Organização na medida em que minimiza a necessidade de recursos para desenvolvimento publicitário. Além disso, os dados pessoais são também uma garantia para estas organizações, visto que, permitem e salvaguardam as empresas de possíveis casos de fraude ou de incumprimento de pagamento.

Não obstante, existem condicionantes intrínsecos ao comércio online de AL, que se refletem num enorme impacto para esta atividade, em particular, no que respeita à segurança e à transmissibilidade dos dados pessoais disponibilizados pelos consumidores.

É certo que, o uso de dados pessoais, contribuiu para a evolução do entendimento pelo gosto, pelas preferências e condutas pessoais dos consumidores, criando oportunidades de negócio ao AL, para que este se torne mais competitivo, facilitando a procura por novas oportunidades fundamentadas na segmentação e na qualidade de serviço.

Embora os dados pessoais revelem ser um dos maiores ativos que possibilite ao AL expandir os seus negócios, informar e divulgar relações segmentadas com os seus clientes, fornecedores, entre outros, conduziu à recolha desmedida de dados pessoais e é, atualmente, uma preocupação a nível global.

Certamente a temática entre a relevância dos dados pessoais para o crescimento das atividades económicas e o direito à proteção dos dados pessoais e à privacidade irá aumentar nas próximas décadas.

Em específico, nas atividades económicas, desenvolvidas em contextos de permanente inovação tecnológica, com serviços que possuem fortes capacidades de recolha de dados pessoais, seja através das aplicações informáticas, dos dispositivos móveis ou de outros dispositivos eletrónicos que incorporam a designada *Internet of Things* (IoT)[7].

A sujeição da aceitação de *Cookies*[8] para usufruir do correto funcionamento do *website*, a possibilidade de existência de vírus ou roubo de identidade, a utilização e aproveitamento de dados pessoais, afetos à obrigatoriedade do acesso à *Internet*, para a realização das reservas *online* são algumas das desvantagens associadas ao AL no digital.

[7] *Internet of Things* (IoT) ou Internet das coisas abrange a globalidade dos aparelhos/objetos que se encontram interruptamente conectados à Internet, conseguem-se identificar na rede e de comunicar entre si, têm a capacidade de recolher uma variada quantidade de informação sobre o que os rodeia.

[8] *Cookies* – Arquivos ou ficheiros de texto, de dimensão proporcional que servem para ser partilhados, de modo célere, através da *Internet* e que dispõem de um conjunto de informações que são armazenadas no dispositivo do utilizador quando este navega numa página *web*.

Mais recentemente e fruto de um fenómeno global pandémico, surge uma enorme ameaça ao setor do AL e uma crise económica sem antecedentes à escala mundial. Com o mundo confinado em casa e sem regular turismo internacional, o AL viu suspendida a sua fonte de rendimento, fazendo do ano 2020 um ano dificílimo.

O surto sanitário provocado pela pandemia de Covid-19 veio afetar o setor do turismo, um dos setores com maior importância para o Produto Interno Bruto (PIB) do país. Segundo o Instituto Nacional de Estatística (INE), Portugal terá uma redução de 2,9% face aos 11,3% que representam o setor do turismo no PIB nacional, o que se traduz numa redução de 25% quer do turismo interno como do não residente.

O AL por ser constituído por micro e pequenas empresas não ficou atrás e foi uma das principais tipologias de alojamento de curta duração a sentir os fortes impactos da pandemia ao nível da faturação. É evidente que estas empresas de acomodação não possuem uma capacidade de resposta equiparável à dos grupos hoteleiros, o que indica que sejam espectáveis quebras de faturação entre 80% e 90% (Neto, 2020).

Em setembro, segundo a estimativa feita pelo INE, 24,3% dos estabelecimentos de alojamento turístico terão estado encerrados ou não registaram movimento de hóspedes e deverá ter assinalado 1,4 milhões de hóspedes e 3,6 milhões de dormidas, o que se traduz em variações de menos de 52,2% e 53,4%, respetivamente face ao período homólogo.

## 2.5 Proteção de Dados

A proteção de dados surge como um fenómeno social extremamente pertinente e preocupante, perante o desenvolvimento tecnológico dos SI e a propensão com que estes meios guiam para a intrusão do sigilo e da privacidade da informação pessoal.

A privacidade está normalmente relacionada às circunstâncias que coloquem em risco a vida privada de um cidadão. Por outro lado, a proteção de dados está associada à recolha e ao tratamento de dados pessoais. Embora sejam conceitos distintos estão implicitamente associados a direitos do cidadão que acabam por estar interligados.

Em conformidade com o n.º 1 do artigo n.º 26 da Constituição da República Portuguesa (CRP), onde se encontra descrita a base jurídica relativa ao direito à privacidade, destaca-se os direitos «à identidade pessoal» e à «reserva da intimidade da vida privada e familiar» de todos os cidadãos. No entanto, é no n.º 2 do mesmo artigo que surge o esclarecimento da CRP através da lei, como meio de garantia e salvaguarda dos direitos dos cidadãos «contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.».

Concomitantemente, a excessiva disponibilização de dados a terceiros, veio fomentar novas e diversificadas vulnerabilidades presentes nos SI, motivo que originou para a necessidade de instituir procedimentos que assegurem a proteção e confidencialidade dos dados. A proteção de dados resulta, em sentido amplo, de uma panóplia de leis e regulamentos adaptados ao longo dos anos por forma a minimizar o risco de apropriação dos dados pessoais da sociedade em geral.

Recentemente, com a aprovação Lei 58/2019, ou como habitualmente é designado por RGPD, foram definidas normas para a proteção de dados pessoais em consequência da frequente utilização de dados que se encontram armazenados digitalmente, que permitem o acesso facilitado a um número incalculável de utilizadores.

Não obstante, a aplicabilidade do RGPD não inclui os dados das pessoas já falecidas, assim como, das pessoas coletivas, com exceção dos dados sensíveis como é o caso de dados genéticos, etnia, filiação sindical. Uma vez que os dados pessoais constituem informações do foro privado de cada cidadão, estes devem ser devidamente definidos para que possam ser preservados.

Segundo o Regulamento (UE) 2016/679, artigo 4º, n.º 1 a definição de dados pessoais consiste em qualquer «informação relativa a uma pessoa singular identificada ou identificável», independentemente do modo como a informação é identificada ou a sua natureza. De acordo com o n.º 26 do Regulamento são também considerados dados pessoais os que tenham sido «pseudonimizados» e «que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares».

A informação pode ser reconhecida diretamente, através de dados de identificação como é o caso do nome, data de nascimento, número de identificação, morada, mas também de modo indireto através de dados de imagem, voz ou dados de localização como é o caso do endereço de IP do computador. O mesmo número não inclui no conceito de dados pessoais as «informações anónimas» em específico as que se destinem para fins estatísticos ou de investigação.

O conceito de dados pessoais é tal modo abrangente que, de facto, alerta para a importância da existência de normas que regulamentem a recolha e tratamento destes mesmos dados. Conforme o estatuído no Regulamento (UE) 2016/679, artigo 4º, n.º 2 esclarece que o tratamento dos dados consiste numa «operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados».

Compreende, por isso, qualquer procedimento que esteja relacionado com o levantamento, análise, registo, uso, divulgação, restrição ou eliminação desses mesmos dados quer seja através de mecanismos informatizados ou manuais.

O tratamento de dados carece da autorização do titular dos dados devendo ser assegurado o direito de conhecimento relativamente à finalidade e propósito a que foram sujeitos e utilizados os dados pessoais, conforme o estatuído no artigo 35º da CRP.

### 2.5.1 A Evolução Legislativa da Proteção de Dados Pessoais

A coesão democrática e económica é uma das razões que se impõe, até aos dias de hoje, como uma das problemáticas mais desafiantes com as quais toda a Comunidade Europeia se confronta. Posteriormente ao término da II Guerra Mundial, surgiu a necessidade de fomentar e salvaguardar os direitos humanos e a democracia por toda a Europa.

Embora não vinculativo, o primeiro exemplar jurídico, a legitimar o direito ao respeito pela vida privada, surgiu em 1948, quando a Assembleia Geral das Nações Unidas celebrou, a Declaração Universal dos Direitos do Homem, no seu artigo 12.º, referindo que «Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação.».

A 4 de Novembro de 1950, com a cooperação de alguns países da União Europeia sob a jurisdição do Conselho da Europa (CDE), foi assinado, em Roma, o primeiro documento jurídico vinculativo, a Convenção Europeia dos Direitos do Homem (CEDH).

De acordo com Saldanha (2019, p.11) «A história moderna da proteção de dados terá início em 1950 [...] tendo por objetivo promover o estado de direito, a democracia e os direitos humanos.». Com o propósito de proteger e honrar, os direitos e as liberdades fundamentais dos cidadãos, foram contemplados no artigo 8.º da CEDH que «qualquer pessoa tem o direito ao respeito da sua vida privada e da sua correspondência só podendo haver interferência se estiver em causa a segurança nacional.».

No contexto nacional, foi pela primeira vez estabelecido o direito à privacidade dos dados pessoais, através da Constituição da República Portuguesa (CRP), de 1976, no seu artigo 35 nº.1 atribuindo a «todos os cidadãos o direito de tomar conhecimento de constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações podendo exigir a retificação dos dados e a sua atualização».

De acordo com Canotilho e Moreira (2014, p.663), o estatuído no artigo 35, dá «a cada pessoa o direito de controlar a informação disponível a seu respeito». Para além disso, este artigo veio instituir limitações ao direito de acesso e à alteração dos dados informáticos, mas também fomentou o direito de sigilo perante os responsáveis e terceiros pelo tratamento de informação automatizada.

A falta de adaptação ao nível da proteção dos direitos pessoais, face às novas imposições legais e simultaneamente, com o aparecimento das TI na década de sessenta, tornou-se inadiável definir mecanismos ao nível do tratamento de dados.

De modo a abranger a maioria dos tratamentos de dados pessoais, o CDE aprovou, em 1981, a convenção 108 cuja aplicabilidade remete para o setor público e privado, que inclui o tratamento de dados sensíveis executados por autoridades ligadas à área da saúde, segurança pública e tribunais tendo em vista a salvaguarda dos direitos dos cidadãos.

Dez anos mais tarde, Portugal ratifica a primeira lei nacional face à informática, a Lei n.º 10/91, de 9 de abril – Lei da Proteção de Dados Pessoais. O princípio geral que rege esta Lei, prende-se no facto de «o uso da informática deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada e familiar e pelos direitos, liberdades e garantias fundamentais do cidadão.».

Através do artigo 2 da Lei da Proteção de Dados Pessoais são estabelecidos conceitos elementares tais como: dados pessoais, dados públicos, sistema informático, ficheiro automatizado, base de dados, tratamento automatizado, entre outros.

É também, a partir desta Lei que surge a Comissão Nacional de Proteção de Dados Pessoais Informatizados (CNPDPI), como entidade de gestão autónoma com autoridade para controlar e fiscalizar o processamento de dados pessoais salvaguardando os direitos, liberdades e garantias do homem presentes na Constituição e na Lei. Posteriormente, passou a designar-se Comissão Nacional de Proteção de Dados (CNPD) e atualmente colabora também na proteção dos direitos de pessoas residentes no estrangeiro, conjuntamente com as autoridades de proteção de dados de outros Estados.

Com o intuito de a harmonizar, as díspares legislações existentes nos estados-membros, respeitantes ao tratamento de dados pessoais e à livre circulação dos mesmos, é então em outubro de 1995, aprovada pela União Europeia (UE) a diretiva 95/46/CE (Diretiva de Proteção de Dados) do Parlamento Europeu e Conselho relativa à proteção das pessoas singulares. Três anos depois, é legislada a nova lei nº 67/98, de 26 de outubro de 1998 – Lei proteção de dados que transpôs para a ordem jurídica portuguesa a diretiva europeia de 1995 e que veio diversificar as funções e competências atribuídas à CNPD.

A Carta dos Direitos Fundamentais da União Europeia (CDFUE), surge em 2000, por forma a complementar toda a legislação até então já aprovada. A CDFUE através do artigo 8 define que «todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito», e que relativamente aos dados estes, «devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei».

Entre os anos de 2000 e 2016 foram aprovadas algumas legislações, em especial o regulamento 45/2001, que veio atribuir regras para a proteção de pessoas singulares no que concerne ao tratamento, à livre circulação de dados pessoais por parte das organizações e órgãos comunitários.

Não obstante, é de salientar que em 2004 a Lei portuguesa nº 43/2004 de 19 de agosto, que veio esclarecer o âmbito de regulação e de atuação da CNPD. No campo de ação da proteção dos dados pessoais, observados pela esfera das forças policiais e judiciais no que concerne a matéria penal, a Decisão-Quadro 2008/977/JAI do Conselho, no ano de 2008, veio definir matéria em área como a liberdade, seguridade e magistratura.

Com a reformulação do *modus operandi* da UE expressa no Tratado de Lisboa, que entrou em vigor a 1 de dezembro de 2009, foi concedido à CDFUE um efeito jurídico vinculativo, em específico, para o respeito pela vida privada e familiar, presente no artigo 7.º e para a proteção de dados pessoais presente no artigo 8.º.

Foi ainda, com o Tratado sobre o Funcionamento da União Europeia (TFUE), artigo 16.º inserida uma base jurídica para a proteção de dados pessoais na UE. Pouco menos de uma década depois, é a 25 de maio de 2018 que entrou em vigor o RGPD (2016/679) que veio revogar a Diretiva n.º 95/46/CE.

Sendo a sua aplicabilidade transversal a todos os Estados Membros da UE, este foi especificamente elaborado para garantir a segurança dos cidadãos face à utilização e tratamento de dados pessoais. Esta revogação, culminou num projeto de continuidade, entre o sistema de proteção de dados presente na diretiva e o novo sistema instituído pelo RGPD, mantendo presente as definições fundamentais como é o caso de dados pessoais, tratamento ou responsável pelo tratamento.

A 12 de junho de 2019, deu-se a aprovação da proposta de lei 120/XIII/3.ª que veio regular a aplicação do RGPD em Portugal, no âmbito em que o próprio determinou serem os Estados Membros a fazê-lo.

Em seguida, a 8 de agosto de 2019, surge a Lei n.º 58/2019 que veio revogar a Lei n.º 67/98, que assegura a execução do Regulamento (UE) 2016/679 relativa à proteção das pessoas singulares no que respeita ao tratamento dos dados pessoais e à livre circulação desses dados. Mas também a Lei n.º 59/2019, que incide sobre as regras de tratamento de dados pessoais respeitantes à prevenção, deteção, investigação ou repressão de infrações penais ou de cumprimento de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Deste modo foi possível garantir a concretização do regulamento (UE) 2016/679, no âmbito jurídico nacional, relativamente à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

### 2.5.2 Regulamento Geral de Proteção de Dados (RGPD)

#### *2.5.2.1 Conceito e âmbito*

Com o propósito de regular a proteção de dados, surgiu a 27 de abril de 2016 o Regulamento (UE) 2016/679, o RGPD, que entrou em vigor a 25 de maio de 2018, como a mais recente alteração no que diz respeito à recolha e ao tratamento de dados de pessoas singulares na UE.

Aprovado pelo Parlamento Europeu e pelo Conselho Europeu, incide sobre os direitos e as liberdades elementares de indivíduos singulares, sobretudo no direito à proteção dos dados pessoais e estabelece as normas respeitantes à proteção das pessoas singulares, ao nível do tratamento e à livre circulação dos dados.

Segundo Couto (2016, p.6) «Este Regulamento dá especial ênfase à livre circulação dos dados permitindo um aumento significativo dos fluxos transfronteiriços de dados pessoais causado pela integração económica e social resultante do funcionamento do mercado interno.». Intervém, ao nível de um variado leque de estruturas públicas ou privadas, que processe ou trate dados de pessoas singulares.

A sua aplicação é transversal a todos os Estados Membros, assegura uma harmonização legislativa, que prevalece sobre quaisquer leis nacionais e coopera para um mercado único europeu de dados, salvaguardado a livre difusão de dados pessoais entre Estados Membros da UE. Para complementar as regras de proteção de dados pessoais já estabelecidas pela Diretiva 95/46/CE, o Regulamento (UE) 2016/679 revogou a diretiva e instituiu algumas alterações por forma a colmatar as lacunas existentes.

Neste sentido, o regulamento intervém ao nível do tratamento de dados pessoais realizado pelo responsável pelo tratamento dos dados e subcontratante, que se encontrem localizados em território europeu, cujas atividades tratam dados pessoais situados dentro ou fora da UE. Segundo Saldanha (2018, p.15), «Verifica-se, portanto, um triplo objetivo que a UE procurou alcançar através deste regulamento: harmonização da legislação, coerência do tratamento de dados pessoais […] e segurança jurídica».

Intervém ainda ao nível de organizações localizadas fora da UE, que ofereçam bens ou serviços a pessoas singulares na zona euro ou que monitorizem a sua conduta dentro do espaço europeu.

Para além de estabelecer um espaço territorial mais ampliado veio ainda aumentar o valor das coimas através da fixação de multas, no caso das empresas, entre 2 e 4 % do volume de negócios anual. Procura ainda definir responsabilidades, estabelecendo a obrigação ao cumprimento do Regulamento (UE) 2016/679 por todos os responsáveis e subcontratantes de dados.

Em conformidade com a Diretiva 95/46/CE, este Regulamento está direcionado para diversas temáticas, entre elas os direitos das pessoas singulares, o respetivo consentimento, o direito de circulação e/ou transferência de dados ou a notificação obrigatória da pessoa aquando da violação dos seus dados pessoais.

Explorando a temática bastante pertinente acerca dos direitos das pessoas singulares, é possível enumerar uma lista com os vários direitos fundamentais, referente à proteção de dados para os quais a sociedade deve estar consciencializada.

Em específico, o direito de informação no que respeita à utilização da informação fornecida à estrutura; o direito de conhecimento, ou seja, de saber quais os dados pessoais que a empresa tem na sua posse e como está a utilizá-los, bem como, o direito de restringir a utilização dos mesmos; o direito à modificação dos dados anteriormente cedidos; e sobretudo o direito à eliminação por parte da estrutura dos seus dados pessoais registados na base de dados, cedidos anteriormente de forma espontânea, caso assim o deseje.

Relativamente ao consentimento da recolha de dados pessoais, deve ter-se em conta a forma de como é feita, a apresentação do pedido e o modo como é solicitado. Este deve ser feito de uma forma simples e clara, por via de uma linguagem acessível e percetível, de maneira que o titular dos dados aquando o pedido não tenha quaisquer dúvidas sobre aquilo que lhe está a ser solicitado.

Entenda-se, consentimento acessível e percetível, como sendo um consentimento através de um documento digital ou em papel, que contenha a identificação da empresa que é responsável pelo tratamento de dados, as finalidades para quais os dados estão a ser recolhidos, a possibilidade de requisitar a anulação do consentimento de recolha de dados, entre outras informações relevantes para que o documento destinado a tal recolha seja sucinto e objetivo. Após o consentimento para a recolha dos dados pessoais, o consentido tem direito ao alerta obrigatório aquando da violação dos seus dados.

As empresas responsáveis pelo tratamento de dados, têm um prazo máximo de 72 horas para notificar a CNPD em Portugal, após a deteção de ocorrência de um caso de violação de dados. «No caso de reclamações ou de violações do Regulamento, estas são da competência da autoridade de proteção de dados do Estado Membro em que ocorram», Fazendeiro (2017, p. 65).

#### *2.5.2.2 Princípios Relativos ao Tratamento de Dados Pessoais*

A carência de uma uniformização ao nível do regime de proteção de dados pessoais, nos países que compreendem o Espaço Europeu que deu origem ao RGPD, veio também apresentar um conjunto de princípios e responsabilidades no que respeita à recolha e ao tratamento de dados pessoais. Na opinião de Fazendeiro (2017, p.67) «as organizações devem implementar medidas técnicas e organizativas de forma a demonstrarem que consideraram e integraram medidas de conformidade com as regras de proteção de dados nos tratamentos de dados que levam a cabo».

Por outro lado, Castro (2005, p.65) salienta para a importância e seriedade com que deve ser feito o tratamento de dados pessoais, sobretudo na «criação» e na «manutenção de um conjunto estruturado de dados pessoais, pelos perigos que pode constituir para os titulares dos dados» considerando esta função como «uma tarefa de responsabilidade».

Estabelece neste sentido, o artigo 5.º do Regulamento (UE) 2016/679 um conjunto de princípios para o tratamento de dados, detalhadamente:

I) Princípio licitude, lealdade e transparência

Este princípio compreende três conceitos para o tratamento de dados pessoais: licitude, lealdade e transparência. Segundo o artigo 5.º, n.º 1, al. a) do RGPD o tratamento de dados pessoais deve ser feito de forma lícita, leal e transparente.

Começando pelo conceito de licitude, segundo Castro (2005, p.235) a «licitude do tratamento é aferida pela verificação do cumprimento das regras nacionais, comunitárias, europeias e internacionais a que este está sujeito», já de acordo com o n.º 1 do artigo 6.º, do RGPD o tratamento de dados só é considerado lícito, quando se verifique pelo menos um dos requisitos elencados nas alíneas deste artigo.

O tratamento é considerado lícito para a concretização de um contrato, conforme regula a alínea b, do n.º 1 do artigo 6.º do RGPD, no qual o titular dos dados é parte ou quando solicitado pelo titular dos dados em situações de diligências pré-contratuais. É um caso que ocorre frequentemente em muitas organizações, nomeadamente no AL, ao nível da recolha de dados de clientes, para elaboração de contratos de AL, pré-reservas ou reservas, contratos de trabalho ou de pessoas envolvidas em processos de recrutamento e contratos de fornecimentos de bens e de serviços com fornecedores.

A alínea c, do n.º 1 do artigo 6.º do RGPD, alerta para o cumprimento de uma obrigação jurídica, como é o caso dos impostos. Neste sentido, uma entidade de AL está obrigada, em sede de IRC, pela Lei n.º 2/2014 de 16/01 a preservar os registos contabilísticos e documentos de suporte, durante o prazo de dez anos e pelo mesmo período em sede de IVA. As faturas das obras ocorridas em imóveis, devem ser conservadas por um tempo mínimo de cinco anos, assim como, os recibos de renda de habitação e os recibos das quotas de condomínio.

Ainda no caso do alojamento turístico, nos termos do artigo 15.º e 16.º da Lei n.º 23/2007, de 4 de julho, é forçosa a recolha de dados para a comunicação de boletins de alojamento, que se reserva a consentir o controlo dos cidadãos estrangeiros e posterior comunicação ao Serviço de Estrangeiros e Fronteiras (SEF).

O consentimento é um dos motivos de licitude e equidade para o tratamento dos dados, o que implica, que sempre que a autorização do titular dos dados for dada sob declaração escrita e que mencione outros temas, o pedido de consentimento deva ser apresentado de forma clara e acessível, permitindo que se identifique facilmente esses outros temas.

É recorrente depender do consentimento dos titulares dos dados, no alojamento turístico, nomeadamente, para os registos dos clientes no *website* para poderem efetuar a reserva, para inquéritos de satisfação na verificação da qualidade de serviço e para efeitos de comercialização e publicidade na comunicação de promoções ou novos serviços.

O tratamento de dados é também, considerado lícito, sempre que, seja indispensável para o desempenho de funções de interesse público ou da autoridade pública, para o efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento, assim como, para a salvaguarda de interesses vitais do titular dos dados ou de outra pessoa singular.

Conforme explica Fazendeiro (2017, p.67) os tratamentos «apenas devem incidir sobre os dados que sejam realmente necessários para a prossecução das finalidades específicas do tratamento.». Importa também que o tratamento seja transparente, no sentido em que, deve respeitar as finalidades para as quais foram obtidos os dados, respeitar o estatuído no regulamento e cumprir com todos os direitos e liberdades dos titulares dos dados.

Por fim no que diz respeito ao conceito de transparência, este em sintonia com os anteriores, rege-se pela relação entre o responsável pelo tratamento e o titular dos dados, através dos direitos do titular dos dados, como por exemplo à informação leal, ao acesso, retificação, restrição e esquecimento dos dados. O tratamento de dados deverá ser transparente para os titulares cujos dados foram reunidos, utilizados, consultados ou sujeitos a qualquer outro tipo de procedimento em que em possam vir a ser tratados.

II) Princípio da limitação das finalidades

Com o excessivo e recorrente tratamento de dados pessoais, tornou-se impreterível definir quais as finalidades para o tratamento dos mesmos e certificar que o mesmo será realizado exclusivamente para a execução dessas finalidades.

Os dados pessoais devem por isso ser reunidos sob uma finalidade específica, clara e lícita, não havendo lugar ao tratamento de dados cujo propósito seja distinto, conforme o estabelecido pela alínea b), do artigo 5 do RGPD. Pinheiro (2018, p.207) considera que «[…] o espaço do princípio da finalidade no direito a proteção de dados pessoais é crucial, na medida em que funciona como a primeira justificação para a realização de um tratamento de dados, impondo-se até ao consentimento.»

Com exclusão, conforme o estatuído no n.º 1 do artigo 89, não é considerado incompatível com as finalidades iniciais, o tratamento subsequente para efeitos de arquivo de interesse público, de investigação científica, histórica ou para efeitos estatísticos. Sempre que se revele para o desempenho de funções de interesse público, é essencial o tratamento de dados tanto a nível europeu como os Estados Membros, podem delimitar e estabelecer os fins para os quais o tratamento subsequente deverá ser classificado compatível e lícito.

No momento do levantamento dos dados das investigações científicas, nem sempre é possível reconhecer na íntegra o intuito do seu tratamento, por esse motivo, os titulares dos dados deverão ter a possibilidade de consentir apenas os seus dados, para determinados âmbitos da investigação científica.

Conforme Pinheiro (2018, p.207) menciona «A realização de recolha de informação pessoal – ou qualquer outra operação de tratamento – deve estar respaldada numa razão-finalidade para, em função dela, se determinar a natureza necessária e não excessiva da informação pessoal recolhida.».

Na eventualidade de se pretender realizar tratamento de dados pessoais, com propósitos diferentes dos quais estes foram reunidos e não exista consentimento por parte do titular para o efeito, o n.º 4 do artigo 6 do RGPD incumbe ao responsável do tratamento de assegurar que este é compatível com os propósitos que deram origem à recolha dos dados.

Pinheiro (2018, p.207) salienta que «A imposição do princípio da finalidade ao consentimento assenta na necessidade de proteger situações em que o primeiro esteja por natureza limitado.». Para atestar a compatibilidade dos propósitos a que está sujeito determinado tratamento, o responsável deverá de ter em consideração o vínculo existente entre o propósito inicial e o propósito subsequente, o contexto da recolha, a natureza dos dados e possíveis posteriores contingências no tratamento dos dados. Contudo, antes da execução do tratamento o responsável deverá facultar ao titular dos dados esclarecimentos sobre esses fins e outras informações relevantes.

III) Princípio da minimização dos dados

Nos termos da alínea c), do artigo 5 do RGPD, o momento da recolha de dados, deve ser direcionado pelo responsável pelo tratamento ou o subcontratante de acordo com o princípio da minimização dos dados. Somente deverão ser recolhidos os dados que se revelem «[…] adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados», consentindo reunir o mínimo de dados possíveis e imprescindíveis para a concretização dos fins.

Segundo Pinheiro (2018, p.209) «é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo.». Este princípio veio reduzir o levantamento desmedido de dados, ou a recolha de dados prescindíveis para a Organização, traduzindo-se numa mais-valia para o titular dos dados, no sentido em que, salvaguarda os seus direitos e liberdades e reduz o risco deste no caso de existir perda de dados.

Deverão ser tratados, unicamente, se o intuito do tratamento dos dados não for possível de ser alcançado, de modo satisfatório, através de outros meios.

IV) Princípio da exatidão

A precisão, autenticidade e atualização dos dados deve ser avaliada mediante o propósito do tratamento. À semelhança do consagrado no artigo 35, n.º 1 da CRP: «Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização», também o princípio presente na alínea d), do artigo 5 do RGPD defende o compromisso da exatidão e atualização dos dados.

Os responsáveis pelo tratamento dos dados e os subcontratantes devem, sempre que necessário, asseverar a concisão e atualização sucessiva dos dados, sendo adstrito a estes o dever de implementar procedimentos e instrumentos que assegurem a remoção de dados inexatos ou desatualizados.

Em harmonia com o artigo 6º, n.º 1 da Diretiva 95/46/CE, devem garantir na recolha de dados, que estes são indicados, relevantes e determinantes para o objetivo do tratamento, assim como, proceder à célere correção dos mesmos sempre que estes estejam incorretos, desajustados ou que tenham sofrido alterações.

Conforme consta no 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.».

V) Princípio da limitação da conservação

O responsável pelo tratamento e o subcontratante devem estabelecer, qual o período indispensável para a preservação dos dados pessoais, no que concerne ao tratamento dos dados pessoais e à consecução dos fins para os quais são tratados.

De acordo com a alínea e), do artigo 5 do RGPD, os dados que possibilitem a identificação dos titulares dos dados devem ser conservados pelo tempo estritamente necessário. Poderão ser conservados por períodos mais longos, os dados que sejam tratados unicamente para fins de arquivo de interesse público, de investigação científica, histórica ou para fins estatísticos sob condição de utilização das medidas técnicas e organizativas previstas no regulamento e restante legislação em vigor.

Em complementaridade, cabe ao responsável pelo tratamento, definir os prazos para a eliminação dos dados, por forma a prestar ao titular dos dados o direito a ser esquecido, conforme o presente no artigo 17º do RGPD.

É também, responsabilidade do responsável pelo tratamento dos dados, a obrigação de apagar os dados do titular, sem demora injustificada, quando a recolha ou tratamento dos dados tenha sido realizada de forma ilícita, os titulares dos dados retirarem o seu consentimento ou se contestarem o tratamento de dados pessoais que lhes digam respeito, ou caso os dados pessoais se verificarem dispensáveis, para o propósito que originou a sua recolha, armazenamento ou tratamento.

Este direito revela especial interesse, quando o titular dos dados tiver dado o seu consentimento ainda em criança e não inteiramente consciente dos riscos associados ao tratamento, existindo a vontade em fase adulta de eliminar esses dados pessoais.

Deverá, por este motivo, ser permitido ao titular dos dados, a possibilidade de exercer o direito à eliminação dos dados.

Finalizado, o responsável pelo tratamento, deverá decidir se o subcontratante devolve ou apaga os dados pessoais afetos ao tratamento, salvo os casos, em que possa ser imposta a preservação dos dados, ao abrigo do direito da UE ou do Estado Membro a que o subcontratante esteja sujeito.

VI) Princípio da integridade e confidencialidade

O princípio da integridade e confidencialidade tem como principal objetivo, preservar a segurança do tratamento dos dados e prevenir que o tratamento de dados viole o presente regulamento. O responsável pelo tratamento ou o subcontratante deve estimar qual o volume de dados recolhidos, a escala de tratamento desses dados, a natureza dos dados, os riscos inerentes ao tratamento e adotar métodos que permitam mitigar os mesmos.

O tratamento dos dados pessoais deve garantir a segurança e proteção dos dados, perante problemáticas como a perda, modificação, danificação ou eliminação quer acidental quer ilegal dos dados e a divulgação ou o acesso indevido a dados pessoais cedidos, preservados ou sujeitos a qualquer outro tipo de tratamento.

Neste sentido, o responsável pelo tratamento deve garantir um nível de segurança razoável, que salvaguarde a integridade e confidencialidade dos dados, conforme o estatuído na alínea f), do artigo 5 do RGPD.

A falta de medidas adequadas e apropriadas, de modo a colmatar estes riscos pode criar oportunidade para danos físicos, materiais ou imateriais como é o caso da privação de autodomínio sobre os seus dados, a extorsão de identidade, roubos financeiros, perda de sigilo de dados ao abrigo do segredo profissional ou qualquer outro dano económico ou social considerável para o titular dos dados. Deste princípio, resulta ainda a obrigação de notificação de violação de dados pessoais, à autoridade de controlo, após ter tido conhecimento do sucedido e sempre que possível no prazo de 72 horas.

Com exceção dos casos, em que o responsável pelo tratamento seja capaz de provar em concordância com o princípio da responsabilidade, que a transgressão não acarreta um risco para os direitos e liberdades dos titulares dos dados.

VII) Princípio da responsabilidade

Com a implementação do RGPD foram feitas alterações face às anteriores legislações, nomeadamente, o fim do pedido de autorização e notificação prévias à CNPD.

O pedido de permissão e a notificação que outrora eram requisitados à CNPD foram substituídos, em concordância com o princípio da responsabilidade, comprometendo o responsável pelo tratamento e subcontratantes de assumirem a responsabilidade pelo cumprimento do regulamento, mas também de apresentar sempre que solicitado, em qualquer momento do tratamento, provas que atestem o cumprimento do regulamento.

É da incumbência do responsável pelo tratamento ou subcontratante assegurar a aplicabilidade dos princípios no que respeita ao tratamento de dados, de acordo com o n.º 2, do artigo 5 do RGPD, assim como, garantir o uso de práticas personalizadas, adaptadas a cada tratamento por forma a atestar que o mesmo é feito em concordância com o disposto no regulamento. É por isso imprescindível, que o responsável preserve a substância, a extensão, o contexto e os propósitos a que se destina o tratamento dos dados.

Segundo o n.º 1, do artigo 24 do RGPD cabe ao responsável pelo tratamento comprovar que, o mesmo é executado cumprindo todas as especificidades deste regulamento, devendo ser em qualquer circunstância capaz de o demonstrar e mostrar provas caso sejam solicitadas. Nos casos de fiscalização a operações de tratamento de dados, os registos de atividades, sob a responsabilidade do responsável do tratamento, devem ser preservados, uma vez que este está obrigado a colaborar com a autoridade de controlo e a facultar-lhe esses registos.

O responsável pelo tratamento, deve instituir procedimentos de promoção e segurança para a proteção dos dados, certificar a conformidade das operações de tratamento segundo o estatuído no regulamento, avaliar os riscos intrínsecos e garantir a sua mitigação, bem como, demonstrar o estado de *compliance* da Organização.

#### *2.5.2.3 Os Direitos do Titular de Dados Pessoais*

O proveito desmedido e a insegurança na transmissão dos dados pessoais, entre as organizações e os agentes económicos até então, vieram com a implementação do RGPD assumir uma maior criticidade por parte dos agentes reguladores e da auditoria no que respeita aos direitos dos titulares de dados pessoais.

À semelhança do que sucedia na Diretiva 95/46/CE, também o Regulamento (UE) 2016/679 elenca os direitos dos titulares dos dados, por forma a garantir ao responsável pelo tratamento de dados e ao subcontratante o correto exercício destes princípios.

I) Direito de Acesso

O direito de acesso confere ao titular dos dados, a asserção por parte do responsável pelo tratamento sobre quais os dados do titular que possui e a respetiva utilização destes perante o tratamento e se for o caso, o acesso aos mesmos.

Ao direito de acesso pode-se associar também, o direito de informação que impõem um conjunto de deveres ao responsável pelo tratamento e de direitos ao titular dos dados. Através da obtenção de informações específicas sobre o tratamento de dados pessoais, rege o n.º 1 do artigo 15.º do RGPD, quais os direitos de acesso do titular dos dados, especificamente:

1. Os motivos pelos quais os seus dados pessoais são tratados, os tipos de dados pessoais que são tratados e os direitos de que goza em relação ao tratamento dos seus dados pessoais;
2. As entidades a quem os dados pessoais podem ser transmitidos, abrangendo as que se localizem em países fora da UE ou organizações internacionais, sendo neste caso comunicado as garantias aplicadas à transferência dos seus dados;

3. Sempre que existam decisões individuais automatizadas, que compreendam a definição de perfis e nessa circunstância, informações sobre a lógica implícita a esse tratamento, bem como, sobre a relevância e os efeitos previstos do mesmo;
4. O período de conservação dos dados ou, caso não se revele possível, os critérios para estabelecer esse período;
5. Nos casos em que os dados pessoais não tenham sido fornecidos pelo titular, as informações sobre a origem dos mesmos;

II) Direito de Retificação

O artigo 16.º do RGPD confere o direito à retificação dos dados pessoais, ou seja, permite ao titular dos dados o direito de solicitar ao responsável pelo tratamento dos dados a correção dos dados pessoais que se encontrem incorretos ou inexatos como é, por exemplo, o caso de uma morada, um número de contribuinte ou contactos.

Face às finalidades do tratamento, o responsável deve proceder à correção dos dados de imediato e caso se justifique, proceder às alterações mediante uma declaração complementar. A título de exemplo, um ciclista despista-se e caí na estrada por causa de um veículo automóvel, pese embora não tenha existido qualquer colisão entre os veículos/condutores, o ciclista apresentou queixa formal e disponibilizou os dados pessoais do condutor às seguradoras.

Em tribunal, o processo judicial determina que não existiu acidente nem que o condutor tenha sido causa do despiste do ciclista. Neste caso, o condutor do veículo automóvel pode pedir às seguradoras que corrija os dados que esta possui a seu respeito para que não seja prejudicado no futuro perante o tratamento de pedidos de seguros.

O responsável pelo tratamento dos dados deve informar as retificações feitas, de acordo com o artigo 19.º do RGPD, a todos os terceiros a quem tenham sido transmitidos os dados, com exceção das comunicações que se revelem impossíveis ou que impliquem um esforço desproporcionado.

III) Direito à eliminação dos dados («direito a ser esquecido»)

Este direito, é como o próprio nome indica, um duplo sentido (eliminação e ser esquecido) que representa a finalidade de dois conceitos, como se de um só conceito se tratasse.

O direito ao apagamento que consta no n.º 1 do artigo 17.º do RGPD, é também mencionado como direito a ser esquecido, no sentido em que reforça e alerta para um maior controlo dos dados pessoais, por parte do titular, no consentimento que este concede face ao tratamento desses mesmos dados.

Castro (2005, p. 239) defende que «O direito ao esquecimento […] obriga a que os dados apenas possam ser conservados de forma a permitir a identificação dos seus titulares durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior». Este direito verifica-se nos dados pessoais, quando estes deixem de ser necessário para a finalidade que justificou a sua recolha, o titular retire o consentimento ou que se oponha ao tratamento, se trate de um tratamento ilícito e se tiver de dar cumprimento a uma obrigação jurídica.

Permite que sejam eliminados dados que o responsável pelo tratamento possua e que já não sejam essenciais para o tratamento, em particular, os dados disponibilizados em criança. Por exemplo, o indivíduo A aderiu a uma rede social aos 14 anos. Anos mais tarde, pretende eliminar a sua conta da rede social e suprimir os seus dados pessoais da base de dados. O indivíduo A possui a possibilidade de exercer este direito independentemente do facto de já ser adulto, visto que consentiu o tratamento dos dados quando era criança e não estava consciente dos riscos intrínsecos ao tratamento.

Perante determinadas circunstâncias, em que o tratamento tenha tornado público os dados pessoais, de acordo com o n.º 2 do artigo 17.º do RGPD, o titular dos dados pode solicitar que os extinga. Para além de eliminar os dados, estão ainda obrigadas a adotar medidas satisfatórias de ordem técnica, tendo em ponderação a tecnologia que está acessível e as quantias da sua aplicabilidade, por forma a comunicar as outras empresas também elas responsáveis pelo tratamento, que procedam à eliminação das ligações de acesso a esses mesmos dados e a eventuais cópias de segurança.

Importa salientar que o direito do apagamento de dados não é um direito absoluto, quer isto dizer, que outros dados devem também permanecer salvaguardados, sendo o seu tratamento necessário e que por essa razão, ao abrigo do n.º 3 do artigo 17.º do RGPD, não está autorizada a eliminação desses dados pessoais.

Como é o caso da liberdade de expressão e informação, da investigação científica, histórica e estatística. Ao fazer uma pesquisa *online* utilizando o seu nome, os resultados expõem uma ligação para um artigo com vários anos respeitante a um assunto processo jurídico resolvido há bastante tempo e que atualmente é irrelevante.

Visto que não se trata de uma figura pública e possui interesse em remover o artigo da pesquisa *online* e caso a sua intenção prevaleça sobre o interesse do público em geral em ter acesso ao artigo, os responsáveis pelo *website* são obrigados a remover os resultados e as ligações para as páginas web que incluam o seu nome.

IV) Direito à Portabilidade

É um dos direitos que surgiu com o RGPD, face à Diretiva 95/46/CE e é possivelmente o direito que mais ativo estará no dia-a-dia dos consumidores, uma vez que possibilita ao titular dos dados, a hipótese de receber e utilizar os seus dados para fins próprios e entre tipos de serviços distintos.

O titular dos dados possui o direito de receber os seus dados, segundo o n.º 1 do artigo 20.º do RGPD, «num formato estruturado, de uso corrente e de leitura automática». Este direito, permite aos titulares transportar, transcrever ou transmitir livremente os seus dados pessoais entre sistemas informáticos ou guardá-los num dispositivo pessoal, onde o titular dos dados possa gerir os seus próprios dados.

Em termos empresariais e exemplificando de acordo com a área de negócio do AL, pode este direito significar que as organizações têm de facultar, quando solicitado pelo titular dos dados, informações ou documentos como é o caso das condições de reserva ou a própria fatura do alojamento. De modo sucinto, Fazendeiro (2017, p.42) explica que a portabilidade «confere aos titulares o direito a solicitarem ao responsável pelo tratamento dos dados, os seus dados pessoais num formato de uso comum e mesmo a sua transferência para outro responsável pelo tratamento».

O direito à portabilidade, pode ser visto como um direito de acesso e de oportunidade que é concedido ao titular dos dados e que garante a transmissão dos dados entre responsáveis, sempre que o tratamento se restringir na base do consentimento expresso, sob execução de um contrato ou mediante meios automatizados.

A título de exemplo, um consumidor que efetue um contrato com a Prestadora A relativo a um seguro de viagens para cobrir eventuais contingências face à sua reserva e que posteriormente pretenda contratar a Prestadora B para adquirir o mesmo seguro, tem como opção exercer o direito à portabilidade. Perante este cenário, ao exercer este direito pode solicitar ao responsável pelo tratamento dos dados da Prestadora A que transmita ao responsável pelo tratamento da Prestadora B os seus dados pessoais.

V) Direito de Oposição

Resulta do direito de oposição, estipulado no n.º 1 do artigo 21.º do RGPD, a permissão concedida ao titular dos dados, de solicitar ao responsável pelo tratamento, a ponderação entre os seus interesses e os interesses do titular viabilizando ao último opor-se, em qualquer circunstância, ao tratamento dos seus dados.

Possui, neste contexto, opor-se ao tratamento dos dados que resultem em finalidades de comercialização direta, de investigação científica e/ou histórica, para recolha estatística, para realização de uma atividade de interesse público ou autoridade pública e ainda, para os seus próprios interesses legítimos.

No caso de se opor à comercialização direta, de acordo com o n.º 2 e n.º 3 do artigo 21.º do RGPD, a entidade está obrigada a cessar a utilização dos seus dados pessoais e a respeitar o seu pedido sem que lhe possa ser cobrada qualquer taxa. Por exemplo, uma pessoa faz uma reserva de 5 noites num AL no Porto através do *Booking*. Depois de efetuar o pagamento recebe inúmeros e-mails de outros alojamentos locais em diversas cidades do país. A pessoa contacta o *Booking* de que não pretende receber mais e-mails publicitários de novas ofertas. Nestas circunstâncias, a empresa deve cessar o tratamento dos dados do titular para efeitos de comercialização direta e posteriormente o consumidor deixar de receber e-mails publicitários.

Sempre que exercido o direito de oposição, os dados serão eliminados, uma vez que não existe outro motivo que justifique o seu tratamento, contudo, a empresa pode prosseguir com o tratamento dos dados pessoais apesar das objeções do titular, quando o tratamento para fins de investigação científica, histórica, estatística, for imprescindível para a execução de uma tarefa por razões de interesse público.

Assim como nos casos em que o tratamento fundamentado em interesses legítimos ou na realização de uma tarefa de interesse público/autoridade pública, evidenciar razões impreteríveis e legítimas que prevalecem sobre os seus interesses, direitos e liberdades.

A empresa deve informar o titular dos dados deste seu direito, quando o contacta pela primeira vez, uma vez que, o efeito do direito de oposição fundamenta-se pela eliminação dos dados, visto que não existe qualquer outro motivo legítimo para a conservação dos dados pessoais.

VI) Direito de Limitação

A restrição do tratamento de dados, subdivide-se ao nível da limitação do âmbito do tratamento a certos grupos/características de dados ou finalidades do tratamento, ou da suspensão das atividades de tratamento.

Possibilita ao titular requerer ao responsável, após um período que permita apurar a fiabilidade dos dados, que delimite o acesso dos dados incorretos ou inexatos.

Prevê a limitação do tratamento nos contextos em que este seja ilícito, nos casos em que o responsável já não necessite dos dados, mas que se revelem fundamentais para efeitos de defesa ou de processos judiciais.

Prevalece também o direito de limitação, pelo período em que o titular apresente renitência face ao tratamento, até que se certifique que os interesses legítimos do responsável se sobrepõem aos seus. No âmbito da limitação do tratamento, conforme o estatuído no n.º 1 do artigo 18.º do RGPD, os dados pessoais só podem, salvo exceção, para o caso da conservação, ser objeto de tratamento com o consentimento do titular.

Por exemplo, o indivíduo A pretende adquirir um crédito à habitação e estuda quais as melhores ofertas prestadas pelos bancos existentes no mercado, ao que verifica que existe outro banco que não o seu com uma melhor oferta. O indivíduo A decide mudar de banco e pede ao antigo para encerrar as contas e que eliminem todos os seus dados pessoais.

Ainda que o banco esteja legalmente obrigado a conservar durante dez anos os dados dos seus clientes, o titular dos dados pode pedir uma limitação ao tratamento dos seus dados pessoais, de forma a assegurar que estes não são empregues para finalidades indesejadas.

#### *2.5.2.4 Decisões Individuais Automatizadas (incluindo perfis)*

As empresas estão permitidas a definir perfis de modo automatizado, computorizando informações pessoais, por forma a analisar e categorizar os clientes, com base nos dados pessoais por eles fornecidos, sem qualquer intervenção humana.

Não obstante, rege o n.º 1 do artigo 22.º do RGPD, o direito do titular «[…] não ficar sujeito a nenhuma decisão, tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.».

Perante decisões que poderão abranger medidas que avaliem aspetos que digam respeito ao titular dos dados, este, deverá ter o direito de não ficar sujeito a tal decisão, sempre que se assente apenas no tratamento automatizado e que crie efeitos jurídicos, que lhe digam respeito ou que o afetem substancialmente de igual modo. Resultam efeitos jurídicos de uma decisão, no momento em que os direitos jurídicos são afetados.

A definição de perfis e de decisões automatizadas são recorrentes no seio das organizações, por mais eficientes que sejam é importante definir e limitar as opções do tratamento. Estes tratamentos automatizados englobam o conceito de perfis, que digam respeito a qualquer forma de tratamento automatizado que avalie características pessoais em particular, a validação e previsão de aspetos associados à situação ou ao desempenho profissional, económico e de saúde, preferências ou interesses pessoais, comportamento, localização e ainda deslocações feitas pelo titular dos dados.

Os titulares dos dados, não devem ser sujeitos a uma decisão sustentada unicamente num tratamento automatizado, este tipo de resolução pode ser consentido, mas com cariz excecional, nos casos em há lugar à permissão por lei da utilização de algoritmos e que consagra as salvaguardas apropriadas.

Adicionalmente, são permitidas as decisões exclusivamente automatizadas nas circunstâncias em que a decisão é indispensável não podendo existir outra maneira de atingir o mesmo propósito. São os casos, em que se dá lugar à comemoração ou realização, de um contrato com o titular dos dados ou nos casos em que o mesmo deu o seu consentimento explícito. Como o das confirmações eletrónicas de reservas de voos ou de AL automatizadas, processos de recrutamento automatizados, recibo de vencimento ou faturas de aquisição de serviços mensais, recebidas via eletrónica, sem qualquer intervenção humana.

Importa mencionar que as deliberações sustentadas por algoritmos, não podem usar categorias especiais de dados, a menos que a pessoa tenha dado o seu consentimento ou o tratamento seja permitido pelos direitos da UE ou em termos nacionais. Por exemplo, o indivíduo A recorre a um banco para tentar obter um empréstimo, no entanto é lhe solicitado que forneça os seus dados, para que o algoritmo do banco o informe sobre a viabilidade da concessão do crédito, indicando a taxa de juro afeta.

Nestes contextos, o indivíduo A deve ser informado pelo banco, que tem o direito de manifestar a sua opinião face à proposta, de a contestar e de requerer que um colaborador do banco faça uma avaliação à proposta apresentada pelo algoritmo.

Para todos os efeitos, qualquer tratamento deverá fazer-se acompanhar das garantias apropriadas, que compreendam informação específica, relativa ao titular dos dados e ao direito de obter intervenção humana, de demostrar o seu ponto de vista, de recolher um esclarecimento sobre a deliberação tomada, no seguimento da avaliação e se for caso disso contestar a mesma.

### 2.5.3 Encarregado de Proteção de Dados (EPD)

Com a evolução tecnológica e o amplo acesso à informação, surgiram novos desafios aos quais, a UE veio tentar dar resposta, em particular à segurança da informação ao nível dos dados pessoais. Após a aprovação do RGPD as organizações, em específico o responsável pelo tratamento, estão obrigadas a nomear um Encarregado da Proteção de Dados (EPD) para a monitorização do sistema de controlo de dados.

Nem todas as empresas necessitam de designar um EPD, em conformidade com o artigo 37.º do RGPD, sem contar com as entidades públicas, à exceção dos tribunais no exercício das suas funções jurídicas, somente as empresas privadas que trabalhem regular e sistematicamente, de forma direta ou indireta, com titulares de dados ou que façam monitorização dos dados em grande escala é que estão obrigadas a implementar este cargo. Assim como, as organizações que registem e analisem características psicológicas e comportamentais nas pessoas ou que trabalhem com dados especiais como a etnia, religião, dados genéticos ou relacionados com condenações penais e infrações.

Todavia, no caso das entidades públicas, pode ser designado um único encarregado para diversas autoridades ou organismos, no entanto é necessário ter em atenção a estrutura organizacional e a dimensão. O mesmo sucede para grupos empresariais, desde que seja possível assegurar facilidade na acessibilidade do encarregado, para a totalidade dos estabelecimentos do grupo.

No caso do AL, conforme clarificado no manual da Associação da Hotelaria, Restauração e Similares de Portugal (AHRESP) (2020), "Manual Prático do RGPD para o canal HORECA", «[…] a obrigatoriedade da nomeação de um EPD não se verifica na grande maioria dos casos do tecido empresarial nacional, constituído por PME's e microempresas». Esta associação essencialmente representada pelos setores da restauração e do alojamento defende que «[…] a necessidade de tratar dados de grande escala não se coloca, nem mesmo ao nível do processamento de dados sensíveis, sendo esse o âmbito da maioria dos associados da AHRESP.».

No entanto, ainda que excluídas dessa obrigatoriedade, recomenda às empresas associadas em que a atividade desenvolvida envolva o tratamento de dados pessoais, designe alguém competente para o cumprimento das obrigações do RGPD.

O EPD deve estar consciente relativamente a todas as questões associadas à proteção de dados pessoais, devendo o responsável pelo tratamento ou subcontratante fornecer, de modo e em tempo oportuno, os recursos indispensáveis à execução dessas funções. É através do responsável pelo tratamento ou o subcontratante que é publicado os contactos do EPD e comunicados à autoridade de controlo.

Determina o artigo 38.º do RGPD, o comprometimento por parte responsável pelo tratamento de dados para apoiar o EPD na manutenção dos seus conhecimentos, bem como, dar-lhe acesso aos dados pessoais e às operações de tratamento em tempo oportuno.

O responsável pelo tratamento e o subcontratante, não podem interferir nas funções do EPD, nem o podem destituir pelo facto de executar as suas tarefas, uma vez que o EPD exerce as suas funções de modo independente. O n.º 4 do mesmo artigo, veio garantir abertura e acessibilidade na comunicação entre os titulares dos dados e o EPD, relativamente a questões associadas ao tratamento dos seus dados pessoais e ao exercício dos direitos que lhe são concedidos pelo regulamento.

#### *2.5.3.1 Funções do Encarregado de Proteção de Dados*

Ao longo dos anos surgiu entre os diversos Estados Membros, a prática de nomear um EPD, embora não estivesse explanada inicialmente na Diretiva 95/46/CE essa obrigatoriedade.

A pessoa responsável pelo cumprimento do RGPD, é denominada em Portugal por EPD, derivado de *Data Protection Officer* (DPO) e é escolhido com base nas suas qualificações profissionais. Embora não seja obrigatório, é recomendável que possua conhecimentos legais e tecnológicos avançados e uma certificação válida que autentique a formação como EPD.

O Regulamento não é estritamente rigoroso no que concerne ao nível de competências que o EPD deve possuir, ainda assim, este fornece informação indispensável relativamente a questões associadas a qualquer tipo de tratamento de dados, colabora e é o elo entre a empresa e a CNPD.

Deve promover a otimização de práticas para o cumprimento das obrigações inscritas no Regulamento e não tem de ser obrigatoriamente um elemento externo, quer isto dizer que, pode ser um colaborador da entidade, responsável pelo tratamento ou subcontratante, ou pode desempenhar funções de acordo com um contrato de prestações de serviços.

Por outro lado, tem a incumbência de transmitir e recomendar ao responsável pelo tratamento dos dados, ao subcontratante e a todos os colaboradores que laborem diretamente com dados, as obrigações compreendidas pelo Regulamento e pelas demais disposições de proteção de dados da UE ou dos Estados Membros.

De acordo com a AHRESP as principais funções do EPD passam por

> « i) informar e aconselhar a empresa sobre a conformidade da proteção de dados; ii) aconselhar sobre a avaliação do impacto da proteção de dados; iii) monitorizar a conformidade da proteção de dados[…]; iv) e cooperar e atuar como ponto de contacto com as autoridades de proteção de dados.».

Segundo o n.º 1, do artigo 39 do RGPD, deve também supervisionar a conformidade e o cumprimento dos princípios pelo qual o regulamento se rege, distribuindo responsabilidades, sensibilizando, fornecendo formação a todos os intervenientes do tratamento de dados e oferecendo apoio às respetivas auditorias.

Adicionalmente, certifica a realização do tratamento e presta apoio ao responsável, quando solicitado, na avaliação do impacto sobre a proteção de dados perante qualquer tratamento, que implique o uso de novos métodos tecnológicos sempre que a sua substância, campo de ação e propósito for passível de originar um alto risco para os direitos e liberdades dos titulares dos dados.

Vinculado ao sigilo e à confidencialidade no exercício das suas funções, o EPD em conformidade com o direito da UE ou dos Estados Membros pode executar outras funções e jurisdições. Compete ao responsável pelo tratamento, nestas circunstâncias, certificar que as funções e jurisdições atribuídas não deem lugar a conflito de interesses.

# 3. Aplicabilidade do RGPD nas empresas de AL

Este capítulo apresenta as metodologias e os procedimentos utilizados ao longo da realização do projeto de investigação, onde se inclui a caracterização da população e a amostra em análise, o processo e período de recolha dos dados, as técnicas estatísticas utilizadas para apuramento dos resultados.

De modo a corresponder ao propósito inicial estabelecido na dissertação foram formuladas questões, por forma a refletir acerca da perceção das organizações de AL sobre a relevância da proteção de dados e do RGPD, tendo em consideração alguns temas, tais como, a importância e o papel do RGPD e do EPD, a respetiva implementação e posterior verificação da conformidade do regulamento face às políticas e procedimentos internos nas organizações de AL.

## 3.1 Metodologias e Procedimentos

Com o avanço das novas tecnologias nas organizações, foram instituídas políticas que carecem de um olhar cauteloso, por parte do auditor, na apreciação da problemática da proteção de dados, em específico na conformidade do RGPD e restante legislação, bem como, no cumprimento dos direitos dos titulares dos dados, na privacidade e segurança no tratamento e gestão de dados pessoais.

Foi neste contexto, que se tomou o ponto de partida para formulação dos tópicos pretendidos para a investigação e posteriormente a realização de uma análise dos dados quantitativa, fundamentada por um inquérito, de modo a dar resposta aos temas em estudo. De acordo com Batista & Sousa (2011, p.53):

> «[…] a investigação quantitativa integra-se no paradigma positivista, apresentando como objetivo a identificação e apresentação de dados, indicadores e tendências observáveis. Este tipo de investigação mostra-se geralmente apropriado quando existe a possibilidade de recolha de medidas quantificáveis de variáveis e inferências a partir de amostras de uma população».

Deste modo numa primeira parte, o objeto de investigação analisa com base nas questões inseridas, de acordo com o modo como o questionário se encontra estruturado.

Em concreto, nos dois primeiros pontos «Contexto da proteção de dados na Organização» e «Encarregado de Proteção de Dados», respetivamente, os conhecimentos específicos das organizações e dos seus colaboradores face ao RGPD e ao EPD.

Com base nestes pontos introdutórios é possível tomar como partida para os últimos dois pontos presentes no inquérito, «Registo e tratamento de dados» e «Consentimento do consumidor», onde se pretende verificar a conformidade das políticas internas destas organizações e se estas possuem mecanismos concordantes com o regulamento.

É importante também comprovar se existe efetividade no cumprimento das políticas por parte da Organização, especialmente no que possa interferir com o cumprimento das normas do regulamento, podendo eventualmente existir, a necessidade de disponibilizar recomendações nos casos em que se revele evidente as inabilidades de cumprir essas políticas, assim como, poderão existir incongruências que deverão ser solucionadas.

### 3.1.1 Definição da População e Amostra

O foco populacional da dissertação tem por base as empresas que operam no ramo do AL incluído os seus colaboradores, quer internos ou externos, que cumprem em simultâneo dois requisitos: possuem e/ou trabalham em estabelecimento de AL em Portugal; possuem e/ou trabalham com dados pessoais em empresas que prestam serviços para organizações de AL.

Estes colaboradores foram selecionados para integrarem a amostra do estudo em virtude de serem os profissionais que atuam diretamente com dados pessoais dos consumidores de AL. Para obter resposta pertinentes às questões basilares da investigação, é necessário que a amostra forneça informação credível e que tenha conhecimento de causa para fundamentar as suas respostas.

Apesar de o número de registos de AL ter tido uma quebra de 40% face ao crescimento verificado em 2018, de acordo com o Registo Nacional de Turismo (RNT), Portugal terminou o ano de 2019 com 91.638 espaços. Tendo por base, os dados disponibilizados no site do Turismo de Portugal, o número possível de respostas a obter seria infindável, mas colocando a hipótese de considerar que por cada registo de AL, existe pelo menos um gestor/colaborador, então o universo de respostas seria no mínimo 91 638 profissionais, considerando assim este número como base para efeitos e cálculos estatísticos apresentados em seguida.

Por forma a viabilizar a análise dos resultados e a extrapolação para a população em causa, estabeleceu-se mediante cálculos estatísticos, a dimensão suficiente da amostra para o presente estudo.

Deste universo somente foram obtidas 136 respostas, das quais apenas 110 foram tidas em consideração para o presente estudo, não por qualquer questão discriminatória, mas por forma a respeitar os requisitos e propósitos anteriormente apresentados, o que equivale, a uma taxa de respostas de 12%.

Na opinião de Sarmento (2013, p. 90-91), «[o] cálculo da dimensão da amostra indica o cardinal dos indivíduos pertencentes à amostra», assim como, «[o] nível de confiança é a probabilidade do Intervalo de Confiança conter o verdadeiro valor do parâmetro».

Ao verificar a adequabilidade da amostra recolhida, para o alcance de conclusões para o estudo e população em análise, é estimado o número mínimo a extrapolar, com um grau de confiança de 90%. Conforme espelhado na Tabela 3.1. o número mínimo de amostra seria de 68 respostas, neste caso foram obtidas 110 respostas o que significa que a amostra recolhida é superior à amostra mínima requerida.

**Tabela 3.1 -** Cálculo da amostra mínima

| **Fórmula de cálculo da dimensão da amostra**<br>n = p(1-p) / [(SE/Z)^2 + (p(1-p)/N)] | |
|---|---|
| **Dados utilizados** | |
| Nível de significância (p-value) | ≤ 5% |
| Nível de confiança (NC) | 90% |
| Variável aleatória nominal padronizada (Z) | 1,65 |
| Precisão (SE) | 5% |
| Probabilidade de sucesso (p) | 50% |
| População (N) | 91 638 |
| **Amostra (n)** | **68** |

Salienta-se que caso o nível de confiança fosse de 95%, com variável aleatória nominal padronizada (Z) de 1,96, a amostra mínima requerida seria de 383 respostas o que representaria um valor bastante superior comparativamente com a amostra recolhida.

Posteriormente foi realizada uma caracterização da amostra em análise, como já referido, constituída por 110 profissionais, cujos dados foram obtidos a partir das respostas à parte inicial do questionário, «Dados Pessoais», onde foram colocadas questões capazes de conduzir à caracterização da amostra.

A Tabela 3.2 sintetiza elementos que caracterizam a amostra em estudo possibilitando observar que 80% dos respondentes, o equivalente a 88 respostas, possui idade igual ou superior a 35 anos e que apenas 16,36% possui idade superior a 55 anos.

**Tabela 3.2 -** Caracterização da amostra

| **Grupo Etário:** | **N** | **%** |
|---|---|---|
| < 25 a 35 Anos | 22 | 20,00 |
| ≥ 35 a 45 Anos | 44 | 40,00 |
| ≥ 45 a 55 Anos | 26 | 23,64 |
| > 55 Anos | 18 | 16,36 |
| **Dispersão Geográfica:** | **N** | **%** |
| Arquipélagos | 25 | 22,73 |
| Norte | 25 | 22,73 |
| Centro | 34 | 30,91 |
| Sul | 26 | 23,64 |
| **Área de negócio em que se insere a organização:** | **N** | **%** |
| Alojamento Local | 78 | 70,91 |
| Gestão Hoteleira | 19 | 17,27 |
| Consultoria e Gestão de Projetos | 3 | 2,73 |
| Contabilidade | 6 | 5,45 |
| Auditoria | 4 | 3,64 |
| **Dimensão da Organização:** | **N** | **%** |
| Micro Entidade | 68 | 61,82 |
| Pequena Empresa | 27 | 24,55 |
| Média Empresa | 10 | 9,09 |
| Grande Empresa | 5 | 4,55 |

Verifica-se ainda que 70,91% das respostas obtidas dizem respeito a sócios, gerentes ou colaboradores que trabalham diretamente no setor do AL e que 29,09% trabalha em empresas de consultoria que prestam serviços a empresas do ramo do AL. Não obstante, 61,82% e 24,55% dos inquiridos respondeu que laboram, respetivamente, para micro entidades e pequenas empresas. Apenas 4,55% trabalha para grandes empresas.

Por outro lado, no que diz respeito à dispersão geográfica, as respostas com base na amostra em análise são muito similares, destacando-se a zona centro que obteve cerca de 8% mais respostas face às restantes zonas.

Salienta-se que para a dispersão geográfica dos Arquipélagos foram refletidas as unidades territoriais dos Açores e Madeira, para o Norte a Região Norte, que abrange distritos como o de Viana do Castelo, Braga, Porto, Vila Real e Bragança, para o Centro foram consideradas as Regiões Centro, Lisboa e Região Sul, foram consideradas também as regiões do Algarve e do Alentejo.

Relativamente às questões que suportam a informação para a caracterização da amostra por atividade em função da faixa etária e da dispersão geográfica, as mesmas poderão ser consultadas no Apêndice 1 da presente dissertação.

De acordo com o Turismo de Portugal e o RNT o setor do AL é constituído maioritariamente por empresários em nome individual ou por micro entidades.

Em conformidade, através de uma análise específica aos dados que definem a amostra é possível depreender que face aos 78 inquiridos (70,91%), que laboram diretamente na área do AL, conforme demonstrado na Tabela 3.3, 56 representam micro entidades e 17 pequenas empresas. Acresce ainda, os 19 inquiridos (17,27%) que operam na área da gestão hoteleira, dos quais 15 dizem respeito a micro e pequenas empresas.

**Tabela 3.3 -** Dimensão das organizações por setor de atividade

| | **Alojamento Local** | **Consultoria e Gestão de Projetos** | **Auditoria** | **Contabilidade** | **Gestão Hoteleira** |
|---|---|---|---|---|---|
| Micro Entidade | 56 | 0 | 1 | 1 | 10 |
| Pequena Empresa | 17 | 2 | 1 | 2 | 5 |
| Média Empresa | 3 | 1 | 0 | 3 | 3 |
| Grande Empresa | 2 | 0 | 2 | 0 | 1 |
| **Total Geral** | **78** | **3** | **4** | **6** | **19** |

### 3.1.2 Recolha dos Dados

A recolha de dados foi feita mediante a elaboração prévia de um conjunto de questões, organizadas por tema e ponderadas tendo em consideração a revisão literária realizada, permitido a formulação de um questionário simples e estruturado capaz de possibilitar que os dados obtidos com carácter quantitativo, viabilizassem analisar uma diversidade de dados e as suas inúmeras interdependências.

Quivy e Campenhoudt (1998, p. 188), defendem a importância da recolha de dados uma vez que passa por:

> «[…] colocar a um conjunto de inquiridos, geralmente representativo de uma população, uma série de perguntas relativas à sua situação social, profissional ou familiar, à sua opinião, à sua atitude em relação a opções ou a questões humanas e sociais, às suas expectativas, ao seu nível de conhecimentos ou de consciência de um acontecimento ou de um problema, ou ainda sobre qualquer outro ponto que interesse os investigadores».

A formulação do questionário requereu a elaboração de um modelo, tipificado como pré-versão, daquilo que seria a versão final após testado e ajustado. Este modelo inicial foi endereçado ao Turismo de Portugal (TP), Associação do Alojamento Local em Portugal (ALEP) e a docentes do Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL), solicitado o seu preenchimento e respetiva interpretação crítica, no que concerne à adequabilidade e compreensibilidade das questões ou outras condicionantes que considerassem relevantes.

Após realizadas as alterações sugeridas, a versão final do questionário, conforme representado no Apêndice 2, foi formulada na plataforma Google Docs – Formulários da Google, estruturado em cinco partes com 28 questões, nomeadamente:

1. Dados Pessoais - Caracterização da Amostra (4 questões);
2. Contexto da proteção de dados na organização – Conceito do RGPD (6 questões);
3. Encarregado de Proteção de dados - Conceito do EPD (6 questões);
4. Registo e tratamento de dados» - Procedimentos Internos (5 questões);
5. Consentimento do consumidor» - Direitos do titular de dados (7 questões);

Para as respostas foram utilizadas diferentes tipologias de questões em específico, questões de resposta única e dicotómica, questões de resposta aberta, escala de Thurstone e escala de Likert.

Por fim, a versão final do inquérito foi enviada à população através de e-mail, tendo início no dia 7 de março de 2020 e término a 20 de abril de 2020.

## 3.2 Análise de Dados

Na opinião de Quivy e Campenhoudt (2005, p. 216) procede-se à observação e respetiva avaliação da informação onde estão incluídas:

> «[…] múltiplas operações, mas três delas constituem, em conjunto, uma passagem obrigatória: primeiro, a descrição e a preparação (agregada ou não) dos dados necessários para testar as hipóteses; depois, a análise das relações entre as variáveis; por fim, a comparação dos resultados observados com os resultados esperados».

### 3.2.1 Análise ao RGPD – Conceito e Políticas Internas

O conhecimento dos inquiridos perante os conceitos associados ao RGPD, foi uma das principais preocupações com a realização do inquérito, no sentido em que o principal objetivo passava por avaliar se as perceções dos inquiridos face aos temas apresentados estavam enquadradas com o legislado pelo regulamento.

Neste sentido, foi questionado aos inquiridos qual o nível de conhecimento da Organização para a qual trabalham, no que concerne ao RGPD e à proteção de dados, assim como, à respetiva implementação e aplicabilidade deste regulamento.

De acordo com o Gráfico 3.1, 47,30% dos respondentes (52) concordam em parte que as organizações para as quais trabalham têm noção sobre o conceito inerente ao RGPD, 30% (33) respondeu que concorda plenamente e não houve qualquer inquirido que discordasse totalmente.


| | |
|---|---|
| Concordo totalmente | 33 |
| Concordo em parte | 52 |
| Não concordo nem discordo | 2 |
| Discordo em parte | 23 |
| Discordo totalmente | 0 |
| **Total Geral** | **110** |

**Gráfico 3.1 -** Conhecimento das organizações face ao RGPD

Face à amostra em análise é possível depreender que a maioria, mais de 75% dos inquiridos, concordam que as empresas para as quais trabalham possuem conhecimento sobre o RGPD, no entanto, importa perceber se os mesmos consideram que os objetivos da Organização estão em concordância com a política de proteção de dados.

Conforme representado no Gráfico 3.2, 40,9% (45) concordam em parte no alinhamento dos objetivos das organizações onde trabalham, com as políticas de proteção de dados instituídas com a legislação do RGPD e 38,2% (42) discordam em parte.


| | |
|---|---|
| Concordo totalmente | 18 |
| Concordo em parte | 45 |
| Não concordo nem discordo | 4 |
| Discordo em parte | 42 |
| Discordo totalmente | 1 |
| **Total Geral** | **110** |

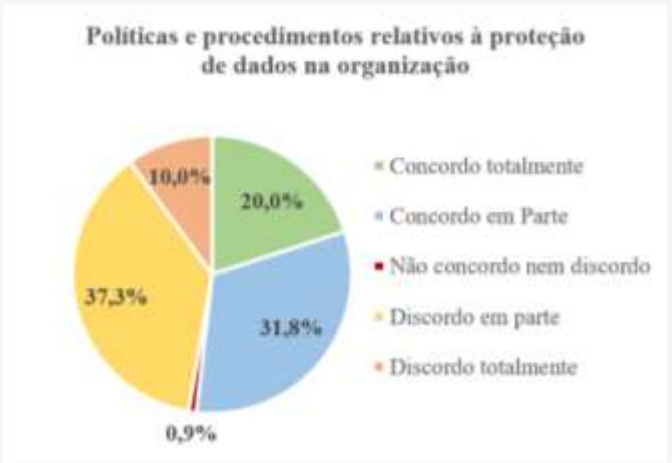
**Gráfico 3.2 -** Objetivos da Organização e a política de proteção de dados

Embora 57,3% (63) das respostas auferidas considerem que os objetivos estão enquadrados com a atual política de proteção de dados, 39,1% (43) diverge dessa opinião. Com base nesta questão e no desenvolver das questões que se seguem é possível assimilar que, apesar das organizações possuírem conhecimentos elementares relativos ao RGPD, muitas destas ainda não adaptaram, na íntegra as suas organizações, por forma a dar resposta às circunstâncias e contextos espelhados no regulamento.

Quando questionados, conforme demonstrado no Gráfico 3.3, com a existência de procedimentos e políticas internas referentes à proteção de dados, no interior da Organização, 51,8% (57) responderam estar de acordo com a existência de políticas e procedimentos, no entanto 47,3% (52) discordaram.

Ora a disparidade que suporta esta diferença de opiniões na amostra em causa é mínima, cerca de 4,5% (5), o que revela que ainda existe uma grande parte de empresas de AL que não possui procedimentos internos adaptados à proteção e privacidade dos dados.

Pese embora a grande maioria destas organizações sejam micro entidades, facto que por essa razão, possuam uma capacidade diminuta na implementação de procedimentos e políticas internas, o Gráfico 3.3, indica ainda que 10% (11) dos indivíduos que responderam ao questionário revelaram estar completamente em desacordo, com o facto de existirem implementadas na Organização, políticas relativas à proteção de dados.




| | |
|---|---|
| Concordo totalmente | 22 |
| Concordo em parte | 35 |
| Não concordo nem discordo | 1 |
| Discordo em parte | 41 |
| Discordo totalmente | 11 |
| **Total Geral** | **110** |

**Gráfico 3.3 -** Políticas e procedimentos relativos à proteção de dados na Organização

A avaliação e o enquadramento dos procedimentos atualmente adotados podem ser feitos com base nas normas, especializações e certificados que as organizações adotem ou possuam e que garantem em parte, conformidade com o RGPD.

É por isso fundamental, que as organizações procedam à revisão e adequação dos procedimentos adotados, pois apenas mediante a realização de uma avaliação de conformidade com o RGPD será, idealmente possível, proceder à adaptação dos procedimentos já existentes e se necessário à implementação de novos procedimentos.

No seguimento da questão anterior, para além da pertinência de apurar se as organizações possuem políticas e procedimentos internos capazes de preservar os direitos e a privacidade dos titulares dos dados, acresce também a importância de compreender qual o nível de preparação tecnológica destas organizações e se estas estão enquadradas com as políticas de proteção de dados.

O Gráfico 3.4 espelha o nível de capacitação tecnológica das organizações no que diz respeito ao RGPD e na opinião dos inquiridos, a preparação tecnológica das organizações onde laboram é inexistente ou mínima. Os dados indicam que 28,2% (31) discorda em parte e 24,6% (27) discorda totalmente. Na generalidade, a maior parte dos inquiridos considera que a tecnologia que existe atualmente nas suas organizações não satisfaz parcialmente os requisitos do RGPD.

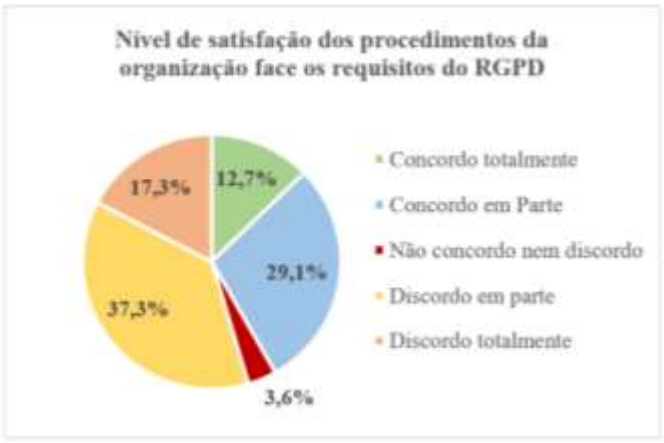

| | |
|---|---|
| Concordo totalmente | 16 |
| Concordo em parte | 26 |
| Não concordo nem discordo | 10 |
| Discordo em parte | 31 |
| Discordo totalmente | 27 |
| **Total Geral** | **110** |

**Gráfico 3.4 -** Nível de preparação tecnológico face ao RGPD

Esta conclusão é rápida de obter comparando os dados obtidos, em que a maioria dos inquiridos discordam com cerca de 52,8% (58), face aos 38,10% (42) que concordam, quer isto dizer que existe, na amostra em estudo, uma incidência preocupante na incapacitação tecnológica das organizações perante a proteção de dados.

Na realidade, o RGPD não elenca medidas técnicas específicas para a adequabilidade e conformidade do regulamento, ou seja, compete às organizações investigarem e determinarem qual o nível de adequação que dispõem e quais as opções e soluções necessárias a implementar.

A existência de procedimentos e políticas não é, por si só, fator que habilite uma Organização a estar em conformidade com o RGPD. Neste sentido, foi questionado à amostra se os procedimentos atualmente adotados na Organização para a qual trabalham satisfazem os requisitos do RGPD. Conforme representado no Gráfico 3.5, 41,8% (46) dos inquiridos concordaram e 54,6% (60) discordaram, sendo que dos inquiridos que discordaram, 17,3% (19) discordam totalmente, comparativamente aos 12,7% (14) que concordam totalmente.




| | |
|---|---|
| Concordo totalmente | 14 |
| Concordo em parte | 32 |
| Não concordo nem discordo | 4 |
| Discordo em parte | 41 |
| Discordo totalmente | 19 |
| **Total Geral** | **110** |

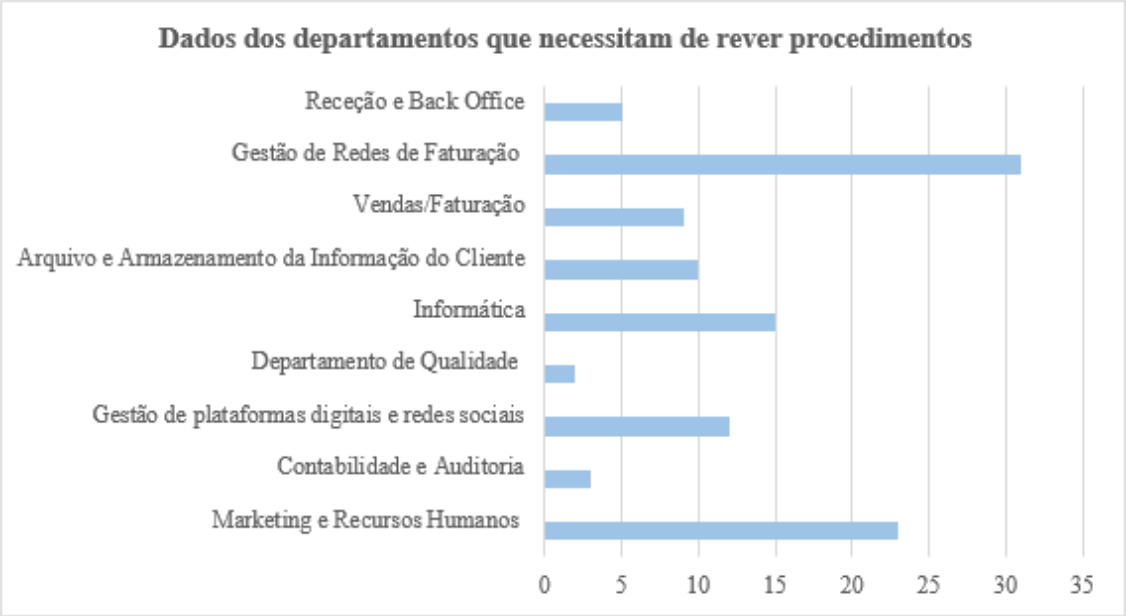
**Gráfico 3.5 -** Nível de satisfação dos procedimentos da Organização face os requisitos do RGPD

A incorporação de procedimentos capazes de estarem em conformidade com a política de privacidade e de proteção de dados, à totalidade dos departamentos existentes numa Organização, assim como, a atualização e automatização dos métodos organizacionais, acresce maior dificuldade para empresas de menor dimensão.

Até porque as organizações com maior dimensão, devido à sua complexidade, possuem uma implementação de condutas rigorosas, quer seja pela necessidade de se adaptar aos públicos-alvo ou pela existência de recursos humanos com díspares ideologias e valências, que cooperam para a criação e entendimento de procedimentos internos.

Importa por isso analisar, com base na análise em estudo, quais os departamentos que, na opinião dos inquiridos, necessitam de implementar processos ou de rever os procedimentos já adotados por forma a que, estes estejam em conformidade com o RGPD, com a proteção e privacidade de dados e que por isso carecem de maior atenção por parte da Organização e da Auditoria.

O Gráfico 3.6 compreende o conjunto de departamentos que no entender dos inquiridos carecem de maior revisão organizacional. Embora esta questão de resposta aberta pudesse suscitar 110 respostas distintas, na verdade a perceção dos inquiridos face aos departamentos mais debilitados foi bastante uniforme, o que permitiu agrupar as respostas obtidas por categorias e retirar os problemas assimilados pelas organizações em análise que são bastante semelhantes.




| | *N* | *%* |
|---|---|---|
| Receção e Back Office | 5 | 0,05 |
| Gestão de Redes de Faturação | 31 | 0,28 |
| Vendas/Faturação | 9 | 0,08 |
| Arquivo e Armazenamento da Informação do Cliente | 10 | 0,09 |
| Informática | 15 | 0,14 |
| Departamento de Qualidade | 2 | 0,02 |
| Gestão de plataformas digitais e redes sociais | 12 | 0,11 |
| Contabilidade e Auditoria | 3 | 0,02 |
| Marketing e Recursos Humanos | 23 | 0,21 |

**Gráfico 3.6 –** Dados dos departamentos que necessitam de rever procedimentos

Da amostra 21% (23) responderam *marketing* e recursos humanos como os departamentos que mais necessitam de rever processos de proteção de dados e 28% (31) respondeu o departamento de gestão de redes de faturação, este último compreende plataformas que procedem à reserva, em alguns casos até mesmo à faturação dos alojamentos dos hóspedes em nome destas empresas, como é o caso do *Airbnb* ou *Homeaway*.

Alguns dos inquiridos, ainda que não tenha sido solicitado, fundamentaram as suas respostas especialmente ao nível dos dois departamentos anteriormente mencionados. As pessoas que responderam alegaram ainda que não tinham conseguido adotar nas suas organizações, uma política de proteção de dados capaz de separar a recolha de dados dos seus hóspedes para efeito de prestação de serviços e de publicidade.

Isto porque, muitos alegam que parte dessa gestão deveria de ser feita pelas plataformas de gestão de reservas visto que são eles que efetuam em primeiro lugar a recolha dos dados pessoais dos hóspedes.

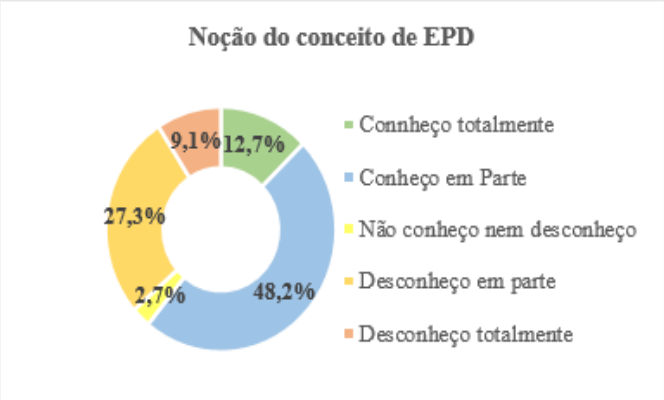
Para além destes, outros departamentos foram mencionados, nomeadamente 8% (9) mencionou o departamento das Vendas/Faturação, 14% (15) o departamento da informática e 11% (12) o departamento de gestão de plataformas digitais e redes sociais.

É percetível que as organizações da amostra em causa possuem dificuldades semelhantes, no entanto, em qualquer dos departamentos da Organização, os direitos dos titulares dos dados devem ser assegurados, desde o direito de notificação, à limitação de tratamento ou até da própria eliminação de dados. Revela-se por isso importante que numa auditoria exista especial atenção às particularidades de cada departamento e proceder a uma avaliação exaustiva dos procedimentos adotados e assinalar quais os que possam estar em desconformidade com o RGPD.

### 3.2.2 Análise ao RGPD – Encarregado de Proteção de Dados

Com a entrada em vigor do RGPD surgiu a figura do EPD, consagrado no artigo 37.º do regulamento, onde estão estabelecidos os casos para os quais as organizações estão sujeitas à obrigatoriedade de designar alguém para exercer as funções de EPD.

Por este motivo, conforme representado no Gráfico 3.7, importa avaliar qual o nível de conhecimento das organizações em estudo sobre o EPD. Segundo as respostas obtidas, 48,20% (53) dos inquiridos assumem em parte que as empresas para as quais trabalham tem noção sobre o conceito de EPD e 12,70% (14) assume conhecer totalmente.



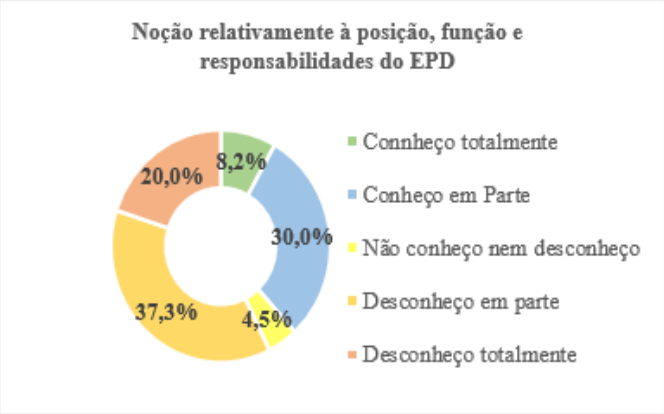

| | |
|---|---|
| Conheço totalmente | 14 |
| Conheço em parte | 53 |
| Não conheço nem desconheço | 3 |
| Desconheço em parte | 30 |
| Desconheço totalmente | 10 |
| **Total Geral** | **110** |

**Gráfico 3.7** - Noção do conceito de EPD

Ainda que face à amostra em observação a maioria tenha respondido de modo positivo, 27,30% (30) respondeu que desconhece em parte e 9,1% (10) desconhece plenamente, o que revela que, parte destas organizações não têm conhecimento sobre o conceito de EPD e que, por causa efeito, desconhecem as suas funções.

Tal é possível de verificar, visto que foi questionado à amostra se esta tinha conhecimento de existir na cultura organizacional, uma definição respeitante à posição, função e às responsabilidades que deverão ser atribuídas a um EPD.

Conforme ilustrado no Gráfico 3.8, 57,3% (63), dos inquiridos afirmam não ter conhecimento, detalhadamente, 37,3% (41) diz desconhecer em parte e 20% (22) diz desconhecer totalmente, quais as funções e responsabilidades que um EPD deve ter. Em contraste, 8,2% (9) respondeu ter plena noção das funções e responsabilidades de um EPD e 30% (33) afirma ter uma noção parcial.



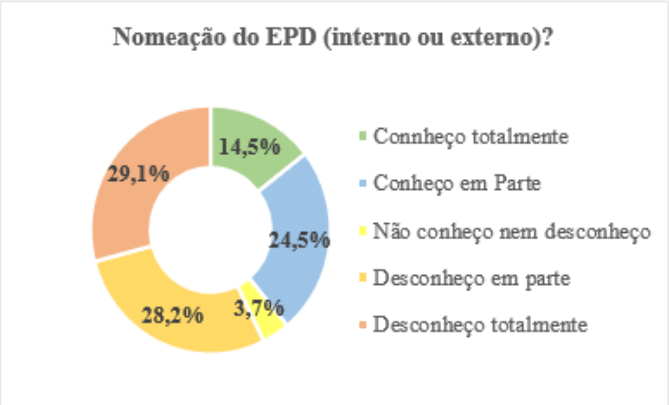

| | |
|---|---|
| Conheço totalmente | 9 |
| Conheço em parte | 33 |
| Não conheço nem desconheço | 5 |
| Desconheço em parte | 41 |
| Desconheço totalmente | 22 |
| **Total Geral** | **110** |

**Gráfico 3.8 -** Noção relativamente à posição, função e responsabilidades do EPD

Salvaguardando melhor opinião, a questão da incumbência da instituição da função do EPD pode suscitar dúvidas ou diferentes tipos de interpretação consoante o responsável pelo tratamento, isto porque no regulamento deveria ter sido feito um esclarecimento adicional, onde mencionasse as causas que incidiram para a origem e instituição da função do EPD e as razões que, inerentes a esta função, acrescem valor às organizações.

Esta obrigatoriedade exige que seja feita uma análise própria e diferenciada a cada Organização. Neste contexto, foi questionado à amostra se tinha conhecimento no interior da própria Organização, existir nomeado formalmente um EPD interno ou externo.

Segundo as respostas obtidas e representadas no Gráfico 3.9, mais de 55% dos inquiridos respondeu desconhecer tal nomeação. Por outro lado, 24,5% (27) respondeu conhecer em parte a existência de um EPD na Organização e 14,5% (16) diz conhecer plenamente, ora isto representa que 39% (43) dos inquiridos tem conhecimento que, dentro da Organização está nomeado um EPD, face aos 57,3% (63) inquiridos que afirma que não existe tal nomeação.

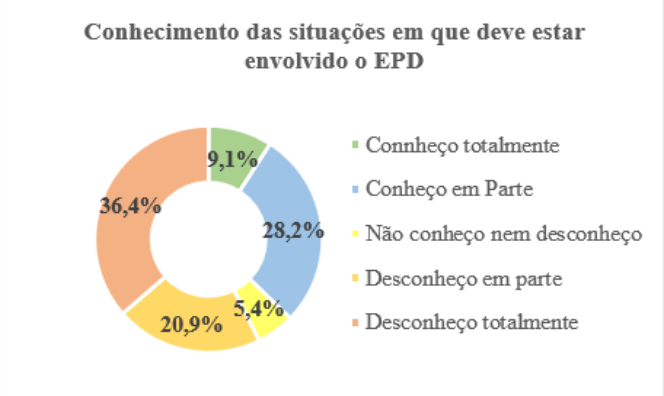



| | |
|---|---|
| Conheço totalmente | 16 |
| Conheço em parte | 27 |
| Não conheço nem desconheço | 4 |
| Desconheço em parte | 31 |
| Desconheço totalmente | 32 |
| **Total Geral** | **110** |

**Gráfico 3.9 -** Nomeação do EPD (interno ou externo)

Adicionalmente, face à realidade tecnológica em que vivemos, o conceito de EPD assim como as suas funções, cumpre o tipo de informação de deverá ser de conhecimento geral a qualquer colaborador de qualquer Organização.

Como exemplificado no Gráfico 3.10 foi questionado aos inquiridos se estes tinham conhecimento, no contexto organizacional, de situações em que o EPD deveria de estar envolvido ao qual 28,2% (31) diz saber em parte e 9,1% (10) saber totalmente.




| | |
|---|---|
| Conheço totalmente | 10 |
| Conheço em parte | 31 |
| Não conheço nem desconheço | 6 |
| Desconheço em parte | 23 |
| Desconheço totalmente | 40 |
| **Total Geral** | **110** |

**Gráfico 3.10 -** Conhecimento das situações em que deve estar envolvido o EPD

Comparativamente aos resultados obtidos na questão anterior, 36,4% respondeu desconhecer totalmente em que circunstâncias organizacionais deverá estar envolvido o EPD e 20,9% diz desconhecer em parte. Os dados revelam, mais uma vez, que mais de 55% da amostra não possui conhecimento suficiente sobre a posição, as funções, responsabilidades e deveres afetas ao cargo de um EPD.

Posteriormente, foi questionado se, no ponto de vista dos inquiridos e do que tinham de conhecimento sobre o tema, o EPD atuava em conformidade com o regulamento ao qual, como demonstrado no Gráfico 3.11, 60% (66) respondeu desconhecer face aos 35,5% (39) que responderam positivamente. Sendo que, destes últimos, apenas 5,5% dizem ter plena noção do plano de ação do EPD e se este está de acordo com o RGPD.


| | |
|---|---|
| Conheço totalmente | 6 |
| Conheço em parte | 33 |
| Não conheço nem desconheço | 5 |
| Desconheço em parte | 26 |
| Desconheço totalmente | 40 |
| **Total Geral** | **110** |

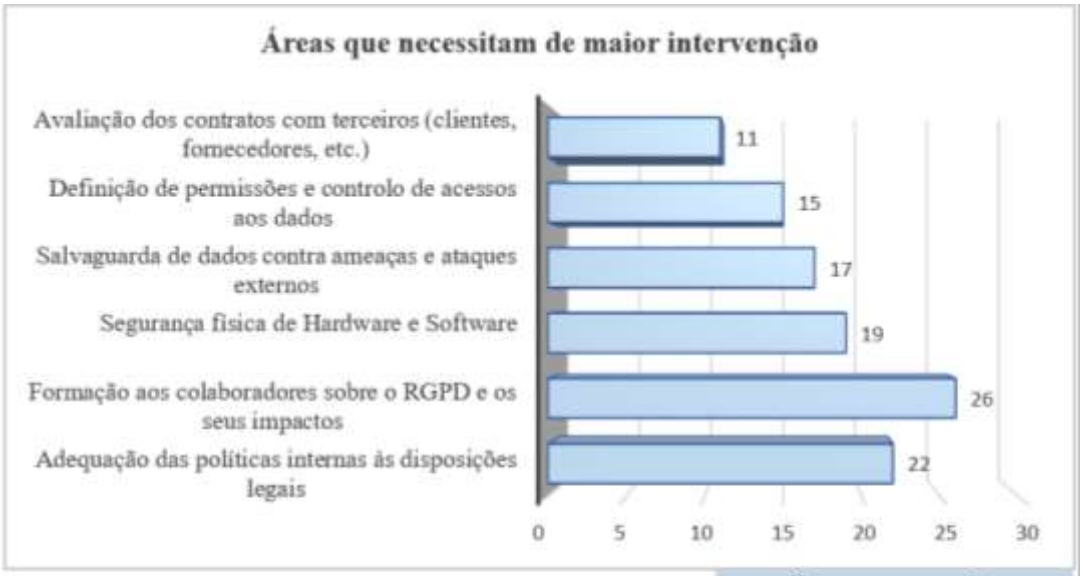
**Gráfico 3.11 -** Conformidade do EPD com o RGPD

De facto, esta questão era um dos pontos chave para atestar a consistência e coerência da amostra, visto que, apenas 39% (43) dos inquiridos tinham respondido ter conhecimento de existir, dentro da Organização para a qual trabalham, a nomeação de um EPD.

Deste modo, as respostas face à conformidade de atuação do EPD com o regulamento estariam, por si só, restritas a esta percentagem uma vez que, se o número de respostas a afirmar «conheço totalmente» ou «conheço em parte» fosse superior aos 39% (43) que afirmaram ter sido nomeado na Organização um EPD, significaria que, muito provavelmente, existiria inconsistência nas respostas obtidas ou que as questões em causa poderiam estar mal colocadas e teriam conduzido a amostra em erro.

Como tal não se verificou, foi possível compreender que 35,5% (39) dos 39% (43) afirmam ter conhecimento em como o EPD da Organização para a qual trabalham atua de acordo com o estatuído no regulamento.

Para finalizar este capítulo do inquérito realizado como exemplificado no Gráfico 3.12, foi colocado à disposição dos inquiridos seis opções conexas a procedimentos internos, especialmente relevantes para a implementação do RGPD numa Organização, com o desígnio de assinalarem qual a opção que consideram precisar de maior intervenção ou, possivelmente, até de ter de instituir dentro da Organização.




| | N | % |
|---|---|---|
| Avaliação dos contratos com terceiros (clientes, fornecedores, ect.) | 11 | 0,10 |
| Definição de permissões e controlo de acessos aos dados | 15 | 0,14 |
| Salvaguarda de dados contra ameaças e ataques externos | 17 | 0,15 |
| Segurança física de Hardware e Software | 19 | 0,17 |
| Formação aos colaboradores sobre o RGPD e os seus impactos | 26 | 0,24 |
| Adequação das políticas internas às disposições legais | 22 | 0,20 |

**Gráfico 3.12 -** Áreas que necessitam de maior intervenção do EPD

Existe uma percentagem significativa dos inquiridos que destacou a formação dos colaboradores relativa ao RGPD com 24% (26) e a adequação das políticas internas ao RGPD com 20% (22) como as áreas que precisam de mais apoio.

A adequação das políticas internas, assim como, as formações são cruciais para uma boa implementação do RGPD. No caso das formações, estas acabam por ser processos de conformidade extremamente importantes para assegurar a política de privacidade e proteção de dados, uma vez que não basta informar os colaboradores, há que dispor de ferramentas organizacionais para os formar. As ações de formação serão sempre essenciais no cumprimento do RGPD, na medida em que, irão sempre existir novas disposições legais, medidas de controlo ou até mesmo decisões judiciais.

Outras duas áreas que se evidenciaram foi a segurança física de hardware e software com 17% (19) e a salvaguarda de dados contra ameaças e ataques externos com 15% (17). De facto, a salvaguarda de dados perante ameaças e ataques internos, mas sobretudo externos, revela-se cada vez mais recorrente e inquietante nas organizações.

A validação aos acessos digitais carece de ferramentas e recursos, como é o caso de palavras-passe, antivírus e backups capazes de salvaguardar a informação, assim como, de garantir que é feito um controlo sistemático aos acessos, possibilitando prevenir futuras situações de fuga ou de roubo de informação.

Embora na opinião dos inquiridos tenha sido uma das opções menos escolhida, com apenas 14% (15), a definição de permissões e controlo de acessos a dados, deve ser tida em consideração de forma rigorosa e criteriosa, uma vez que deve asseverar que exista dentro da Organização, uma base estrutural de cargos hierárquicos, capaz de segregar funções e acessos por forma a preservar a privacidade e segurança dos dados, assim como, os princípios da minimização e limitação de dados.

Visto que a atividade de AL é uma área que está afeta a uma diversidade enorme de recolha e tratamento de dados, caberá depois aos auditores analisar, quais as áreas mais deficitárias em termos de medidas adotadas pela Organização e pelo responsável pelo tratamento de dados sempre que seja necessário, sugerir a adoção de outros procedimentos.

### 3.2.3 Análise ao RGPD – Registo e Tratamento de Dados

Atualmente a complexidade das empresas, independentemente da sua dimensão, obriga a que seja instituído um conjunto de ferramentas para que, de forma estruturada e clara, todas os intervenientes estejam em sintonia, que saibam quais as suas funções e os procedimentos internos da Organização por forma a conseguir compreender se os mesmos estão em conformidade com o RGPD e com a política de proteção de dados.

A verificação e análise das políticas corporativas, referentes ao registo e tratamento de dados pessoais que existem numa empresa, é um dos pontos mais cruciais do plano de trabalho de uma auditoria, na medida em que, permite aferir o nível de conformidade de uma Organização com o regulamento. Neste sentido, foi questionado à amostra qual o nível de adaptação dos procedimentos internos face às políticas impostas no regulamento.

De acordo com o Gráfico 3.13, 67,3% da amostra considera que já existe, nas empresas onde labora, procedimentos internos de acordo com a proteção de dados, especificamente, 22 dos inquiridos, que correspondem a 20% da amostra, responderam que existe um conjunto de políticas implementadas de acordo com o RGPD e 52 inquiridos, 47,3% da amostra, afirmam que as políticas da empresa estão pontualmente de acordo com o regulamento em análise. Ainda assim, 21 dos inquiridos, com 19,1%, afirma não existirem formalizados procedimentos de acordo com o RGPD.

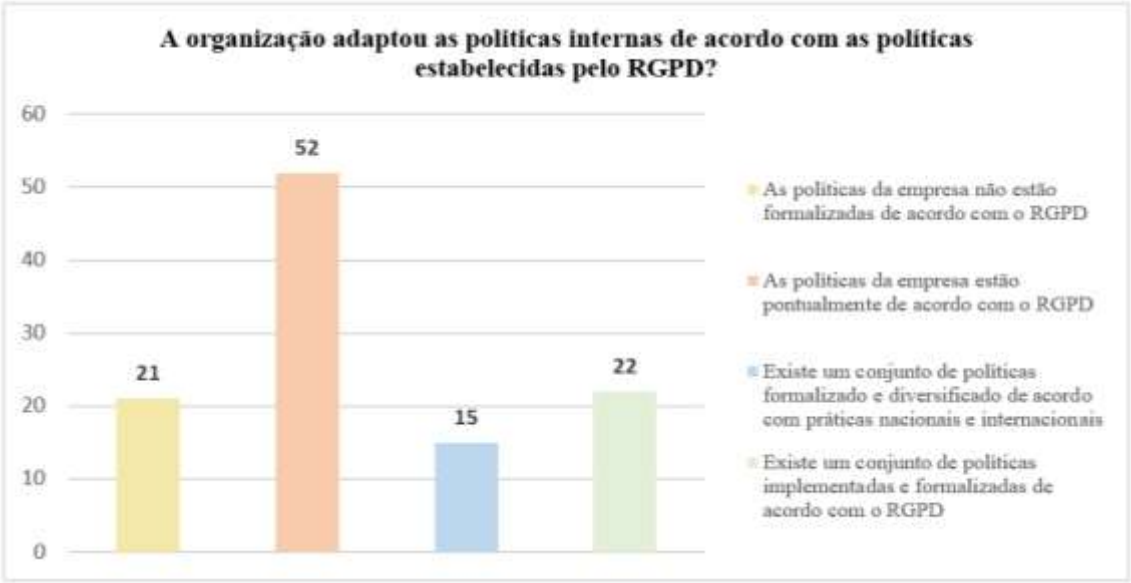



**Gráfico 3.13 -** Adaptação das políticas internas com o RGPD

A implementação de políticas internas exige uma revisão exaustiva das necessidades e funções de cada departamento pois, conforme a especialização de cada área da Organização, serão assim enquadradas medidas a desenvolver.

Por exemplo, no departamento de reservas será imperioso rever os métodos afetos à gestão das plataformas digitais que controlam as reservas e os respetivos pagamentos, aos próprios e-mails nos casos em que os hóspedes tenham feito a reserva diretamente com o alojamento, analisar propostas para alojamento de grupos, examinar o manual de procedimentos e verificar se este está atualizado e de acordo com as políticas de proteção de dados, entre outros.

Neste sentido e em seguimento da questão anterior, foi inquirido à amostra como representado no Gráfico 3.14, se esta considerava ser necessário reajustar os processos de proteção de dados adotados nos diversos departamentos das organizações, ao qual 42 (38,18%) dos inquiridos afirmou serem necessárias algumas correções nos processos existentes e somente 5 (4,5%) consideram não serem necessárias correções.

Em contraste, 34 (30,90%) dos inquiridos consideram serem necessárias muitas correções nos processos existentes e 29 (26,36%) afirma mesmo ser necessário criar processos de proteção de dados.

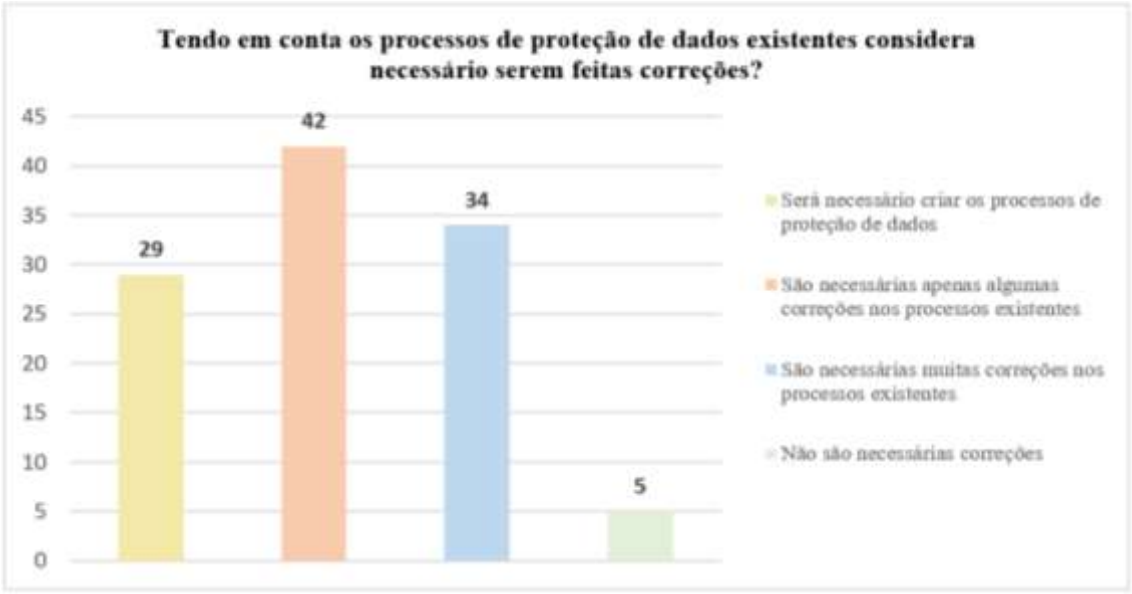



**Gráfico 3.14 -** Necessidade de corrigir os processos face ao RGPD

Nem sempre as empresas conseguem fazer uma correta implementação das políticas internas inerentes à proteção de dados por falta de meios ou ferramentas adequadas, em muitos casos utilizam sistemas já ultrapassados face à atualidade tecnológica em que vivemos ou sistemas sem qualquer tipo de proteção face a ameaças exteriores.

A segurança da informação é um dos principais focos com o qual se baseia a regulamentação do RGPD, independentemente da dimensão ou atividade da Organização. É certo que quanto maior for a Organização mais mecanismos serão necessários de implementar, uma vez que maior será o número de pessoas a registar e tratar os dados.

Entende-se que a segurança da informação passa sobretudo pela elaboração e implementação de procedimentos internos e pela formação que é dada a todos os intervenientes da Organização.

É por isso que associado aos procedimentos internos, importa definir o nível de capacitação das organizações face à proteção de dados, no que respeita à gestão de acessos, conforme representado no Gráfico 3.15.

Surpreendentemente, 47 (42,72%) dos inquiridos afirmam que as organizações onde trabalham não estão preparadas, em ambos os sentidos, para gerir os acessos aos dados pessoais e 32 (29,09%) afirmam que as organizações onde laboram estão substancialmente mais preparadas para a gestão do acesso físico do que do digital.

Somente 17 (15,45%) dos inquiridos respondeu considerar que a Organização está substancialmente mais preparada para a gestão de acessos digitais do que físicos e apenas 14 (12,72%) considera que a Organização onde trabalha está substancialmente preparada tanto para o acesso físico como para o acesso digital.


**Gráfico 3.15 -** Gestão de acessos de acordo com o RGPD

O incumprimento do RGPD não é apenas responsabilidade dos recursos técnicos ou da administração, mas sim de toda a Organização. Nesse sentido, para encerrar esta observação associada ao questionário realizado foram introduzidas duas questões à amostra inicial.

Especificamente, numa situação de incumprimento há conhecimento das penalidades existentes e ainda, se no caso de haver uma inspeção, se consideravam que a empresa poderia sofrer uma penalização.

De acordo com o Gráfico 3.16 é possível verificar que a maioria, mais concretamente 53 (48,18%) dos inquiridos, afirmam ter conhecimento da existência de penalizações, mas desconhecem os montantes.

No entanto, com percentagens muito semelhantes 18 (16,36%) revelam ter conhecimento das penalidades, bem como, os montantes máximos e mínimos previstos na lei. Por sua vez, 20 (18,18%) dos inquiridos dizem ter noção das penalidades, mas apenas tem conhecimento dos montantes máximos previstos na lei. Em oposição, 19 (17,27%) dos inquiridos indicou não ter qualquer conhecimento relativamente à existência de penalidades no incumprimento do RGPD.

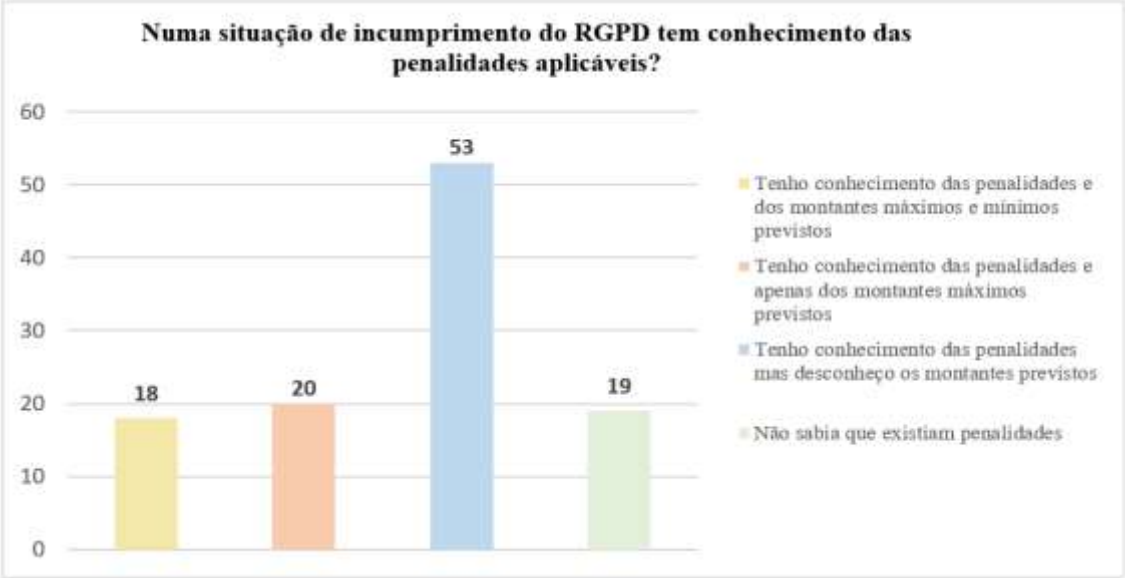



**Gráfico 3.16 -** Penalidades no incumprimento do RGPD

No que diz respeito às penalidades, 30,1% da amostra afirma não saber se a sua empresa sofreria uma penalização financeira com a aplicação do RGPD. Por outro lado 23,6% afirmam que não seriam penalizados e contraditoriamente, 37,7% revelam que muito provavelmente seriam penalizados.


| | N |
|---|---|
| Sim | 41 |
| Não Sei | 43 |
| Não | 26 |
| **Total Geral** | **110** |

**Gráfico 3.17 -** Aplicação de coimas no RGPD

Importa salientar que face às respostas obtidas, é evidente que existe uma grande incerteza na avaliação da possibilidade de serem aplicadas penalizações, sobretudo, devido à imprecisão existente em alguns aspetos referentes ao RGPD, nomeadamente, no que diz respeito à implementação e adequabilidade dos procedimentos internos e à segurança dos dados.

### 3.2.4 Análise ao RGPD – Princípios e Direitos do Titular dos Dados

Nesta fase do inquérito foi utilizada a escala de Likert, por níveis de concordância e discordância, começando em 1[9] para as circunstâncias com as quais os inquiridos discordam totalmente, até 7 representando assim as situações em que concordam totalmente.

Conforme representado na Tabela 3.4, foram colocadas sete questões referentes aos princípios e direitos dos titulares dos dados estatuídos pelo RGPD, tendo em conta as atividades das organizações, onde a vermelho se encontra salientado, para cada questão, o nível com maior percentagem de respostas obtidas.

Face às questões colocadas aos inquiridos nesta fase do inquérito houve uma notória acentuação das respostas para o ponto 2 com a resposta "discordo parcialmente". Também para os restantes níveis de resposta, houve uma grande similaridade de respostas por parte dos inquiridos, quer isto dizer que, numa amostra de 110 inquiridos as respostas nesta fase do inquérito foram em grande parte muito semelhantes.

[9] Escala utilizada: 1- Discordo totalmente; 2-Discordo parcialmente; 3-Discordo; 4- Não concordo nem discordo; 5- Concordo parcialmente; 6- Concordo; 7-Concordo totalmente

**Tabela 3.4 -** Princípios e direitos do titular dos dados

| Questoes | Respostas | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | |
| | N | % | N | % | N | % | N | % | N | % | N | % | N | % |
| 1. Estão definidos dentro da organização procedimentos para a obtenção de consentimento junto do consumidor? | 7 | 6,40% | 40 | 36,40% | 13 | 11,80% | 9 | 8,20% | 20 | 18,20% | 12 | 10,90% | 9 | 8,20% |
| 2. Os responsáveis pelo tratamento aplicam medidas técnicas para assegurar que, em regra, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento? | 6 | 5,50% | 26 | 23,60% | 26 | 23,60% | 17 | 15,50% | 17 | 15,50% | 12 | 10,90% | 6 | 5,50% |
| 3. As medidas aplicam-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento e ao seu prazo de conservação ? | 12 | 10,90% | 27 | 24,50% | 17 | 15,50% | 17 | 15,50% | 17 | 15,50% | 13 | 11,80% | 7 | 6,40% |
| 4. Os procedimentos adotados asseguram que, em regra, os dados pessoais não sejam disponibilizados a um número indeterminado de pessoas singulares? | 11 | 10,00% | 26 | 23,60% | 17 | 15,50% | 20 | 18,20% | 12 | 10,90% | 14 | 12,70% | 10 | 9,10% |
| 5. Nas atividades de recolha e registo de dados pessoais é fornecido a identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante? | 10 | 9,10% | 31 | 28,20% | 15 | 13,60% | 20 | 18,20% | 14 | 12,70% | 11 | 10,00% | 9 | 8,20% |
| 6. Quando os dados pessoais não são recolhidos junto do consumidor, o responsável pelo tratamento informa quais as finalidades do tratamento a que os dados se destinam? | 16 | 14,50% | 28 | 25,50% | 16 | 14,50% | 23 | 20,90% | 15 | 13,60% | 5 | 4,50% | 7 | 6,40% |
| 7. Existem procedimentos de validação relativamente à obtenção dos consentimentos dos dados dos consumidores? | 20 | 18,20% | 31 | 28,20% | 15 | 13,60% | 13 | 11,80% | 18 | 16,40% | 6 | 5,50% | 7 | 6,40% |

Deste modo é possível retirar duas observações. Em virtude de a amostra em causa ser maioritariamente constituída por micro entidades, remete-nos para que face às condicionantes existentes na atividade do AL, os problemas são transversais às organizações em estudo.

Adicionalmente, perante as questões práticas do RGPD revela-se uma enorme inexistência de políticas internas e de conhecimento sobre o tema em análise. Como tal é possível retirar, face a uma escala de 1 a 7, a existência de uma percentagem significativa de respostas com o nível 4, em que não possuem opinião sobre o tema.

Poderá também equacionar-se se a escala de Likert não terá sido, possivelmente, a melhor opção de resposta para as questões apresentadas nesta parte do questionário. Neste sentido e tendo em consideração a incerteza atribuída às respostas nesta fase de apuramento dos resultados, o questionário não foi tido em consideração, situação díspar face às fases anteriores.

# 4. Contributos para a monitorização e realização de Auditorias ao RGPD nas entidades de AL

Perante a atual Sociedade de Informação onde, em cada segundo, são recolhidos, armazenados e suprimidos dados, as empresas têm vindo a procurar saber quais os padrões de consumo e preferências dos seus clientes de modo a conseguir incrementar as suas vendas. Intrinsecamente a esta procura, acresce o número de dados pessoais recolhidos, tratados e armazenados aumentando drasticamente os riscos associados à utilização de dados pessoais. De acordo com o preâmbulo do RGPD:

> « [a]s pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União Europeia e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.»

Neste contexto, têm surgido diariamente novos métodos de recolha e armazenamento de dados e que através dos novos sistemas tecnológicos revelam ser cada vez mais intrusivos. Este tema tem suscitado inúmeras dúvidas e questões, sobretudo ao nível da segurança de dados, facto que carece cada vez mais da intervenção da auditoria e desta atestar os procedimentos adotados e mediante as suas avaliações reduzir os riscos intrínsecos à atividade de AL.

Com base nos resultados obtidos no inquérito, analisado no Capítulo 3, instituir uma correta política de proteção de dados pessoais somente com base nas grandes organizações ou naquelas cuja atividade se dedique à recolha e tratamento de dados revela-se insuficiente, uma vez que todas independentemente da sua dimensão recolhem e tratam dados pessoais e por vezes até dados sensíveis que são geridos por plataformas internacionais. De facto, a generalidade das entidades de AL caracteriza-se como micro ou pequenas empresas, razão pela qual não estão obrigadas a algumas das especificidades estatuídas no RGPD.

Não obstante, não é possível descredibilizar os enormes volumes de dados pessoais que operam diariamente nem os riscos que daí sucedem. Importa por isso destacar alguns dos muitos contributos para a monotorização e realização de auditorias ao RGPD nestas organizações.

Complementarmente, a necessidade de atuação da auditoria nestas pequenas organizações não "vigiadas" no que diz respeito à problemática do RGPD no AL, evidenciando mecanismos de monotorização que poderão ajudar a mitigar partes das lacunas existentes na aplicabilidade e no cumprimento deste regulamento.

## 4.1 Auditoria ao RGPD no Alojamento Local

A evolução da economia digital e do turismo suscitaram novos desafios na área de negócio do AL, especificamente, ao nível do RGPD e da proteção de dados pessoais.

Após a aprovação do regulamento, surge a necessidade de efetuar analises recorrentes face à proteção de dados e à adoção de métodos que certifiquem a realização de medidas corretivas, capazes de preservar os direitos dos respetivos titulares, assegurando a existência de controlos e validações às regras vinculativas aplicáveis a estas organizações.

De modo geral, a auditoria para além de ter de estar em permanente atualização sobre o progresso dos sistemas tecnológicos das organizações, deverá independentemente do grau de complexidade ou tamanho da Organização, passar a contribuir para a realização de apreciações de impacto, relativamente à proteção de dados.

Deve por isso ter cuidados redobrados no que diz respeito aos SI, procedimentos e processos internos que interfiram com a recolha e tratamento de dados face às imposições inerentes ao RGPD.

É por isso importante promover a otimização de práticas e o cumprimento das obrigações inscritas na legislação em vigor. O papel da auditoria ganha assim uma nova direção e importância, na medida em que é, imprescindível, a realização de auditorias competentes e personalizadas à matéria, capazes de estabelecer medidas corretivas adequadas de modo a assegurar conformidade nos procedimentos internos das organizações.

Por este motivo, como em qualquer auditoria de conformidade, é necessária uma preparação prévia, com base numa recolha de dados da Organização em causa, por forma a conhecer a área de negócio desenvolvida, neste caso a atividade de AL, identificar qual o tamanho da Organização, o número de funcionários, os departamentos existentes e ainda que de modo superficial qual a relação dos departamentos com os dados pessoais.

Releva-se sobretudo como um imperativo, compreender o comprometimento da Organização para com a proteção dos dados pessoais que recolhe e trata, o conhecimento que esta possui relativamente às disposições legais em vigor e da necessidade da Organização ter de se adaptar para o cumprimento do RGPD.

Uma vez que se trata de uma primeira apreciação torna-se pertinente entender mediante um conjunto de questões/temas a relação e conduta da Organização com a proteção de dados pessoais, especificamente:

I) Verificar se existe uma chefia responsável pela gestão e proteção dos dados pessoais aos quais a Organização tem acesso;

II) Identificar os departamentos que recolhem, tratam, guardam, partilham e que intervém ao nível das cópias de segurança e da eliminação de dados pessoais, assim como, os responsáveis por esses departamentos;

III) A Organização tem definido um departamento ou um responsável pelo cumprimento e garantia dos direitos dos titulares dos dados;

IV) Existem na Organização representantes dos titulares dos dados e com que periodicidade efetuam reuniões sobre o tema da proteção de dados e da privacidade;

V) Entender se no interior da Organização existe a figura de EPD, se executa exclusivamente a função de EPD, se foi formalmente designado para o cargo;

VI) Compreender se existiram ações de formação relativamente à proteção de dados e se estas foram dadas a globalidade da Organização ou apenas a alguns departamentos em específico;

VII) Identificar se existem políticas para a realização de formulários dentro da Organização sobre a proteção de dados, quem realiza esses formulários e quem valida a sua conformidade com o RGPD;

VIII) Os códigos de conduta da Organização foram adaptados e estão em conformidade com o RGPD, as políticas internas foram reajustadas e implementadas de acordo com os critérios vigentes, preservam a proteção de dados e a privacidade dos titulares;

IX) Face aos procedimentos internos e técnicas organizativas, quem averigua o respetivo cumprimento do RGPD, a segurança do tratamento dos dados e com que periodicidade são feitas essas avaliações;

X) Conferir se existem notificações ou consultas efetuadas à CNPD assim como se foram feitas anteriormente auditorias ao tratamento da informação.

Estes tópicos embora introdutórios, são pertinentes de serem colocados posteriormente a cada departamento/chefia por forma a assegurar uma confiança razoável ao auditor de que possui um conhecimento aprofundado sobre a ligação da empresa com a recolha, partilha e tratamento dos dados pessoais. Ainda assim, é fundamental definir por departamento, quais os funcionários que devem estar presentes, por forma a poder obter respostas credíveis e fundamentadas sobre os tópicos apresentados.

Posteriormente, em semelhança com qualquer outra auditoria ao RGPD, segue-se a fase do planeamento que deve ter por base uma sequência de métodos e ferramentas capazes de dar resposta aos procedimentos implementados dentro da Organização. De modo sucinto, é possível englobar e subdividir o planeamento e a áreas de atuação da auditoria em quatro fases, conforme é representado na Figura 4.1.

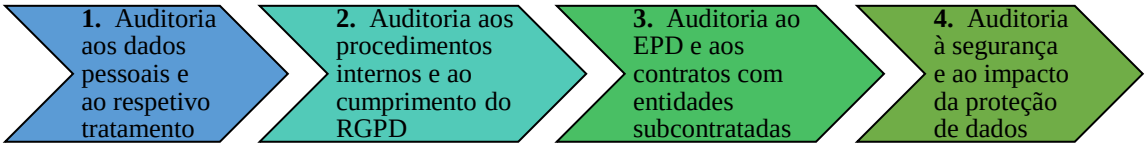



**Figura 4.1-** Fases do planeamento de uma auditoria interna à implementação do RGPD

Na verdade, todas estas fases de planeamento têm como propósito garantir a plenitude e confidencialidade no que diz respeito à segurança dos dados pessoais, aferir a licitude da recolha, partilha e tratamento dos dados, assim como, aquilatar a eficiência e eficácia do sistema de controlo interno e a conformidade dos procedimentos adotados pelas organizações com a legislação vigente.

### 4.1.1 Auditoria aos Dados Pessoais e ao Respetivo Tratamento

Na realidade da indústria turística, como é o exemplo do AL, desde sempre que as suas atividades estiveram afetas à recolha e ao tratamento de dados pessoais dos seus consumidores para a execução das suas prestações de serviço.

É evidente que o trabalho do auditor tem sempre, mas sobretudo quando respeita à proteção de dados, de ser reajustado à área de negócio em que a Organização se insere e a partir de determinado procedimento/fase definir quais os pontos fulcrais a verificar.

Releva-se por isso necessário, categorizar por tópicos desde o princípio de uma auditoria, quais os postos-chaves relativos à gestão e ao tratamento de dados carecem de uma avaliação e apreciação mais detalhada por parte dos auditores. Resumidamente:

I) Enquadrar o tamanho da Organização (micro, pequena, média ou grande empresa) e perceber se esta está preparada e se tem capacidades para gerir o acesso e tratamento dos dados pessoais (quer em formato digital como físico);

II) Identificar quais as áreas de negócio em que a Organização recolhe e trata dados pessoais (Faturação, Recursos Humanos, entre outros) e quais as finalidades do negócio que exigem a recolha e o tratamento dos mesmos;

III) Compreender, como é que Organização executa o tratamento de dados, se por meios totalmente ou parcialmente automatizados ou não automatizados, assim como, se a recolha e o tratamento são executados pela própria Organização ou se requer entidades subcontratadas (terceiros) para a execução destes procedimentos;

IV) Analisar o modo como é feita a recolha e o tratamento de dados, se esta vai de encontro com a natureza, âmbito e finalidades ou se é restringido segundo a religião, etnia, ações penais e/ou infrações do titular dos dados, bem como, avaliar se o tratamento dos dados da Organização requer um controlo contínuo e sistemático dos dados em grande escala;

V) Averiguar se a Organização executa tratamentos com base em definição de perfis, ou seja, se usa os dados pessoais para aferir determinadas características pessoais de um titular de dados, com o propósito antecipar características relacionadas com o cargo profissional, situação econômica, saúde, gostos pessoais ou localização.

No caso do AL, devido à diversidade geográfica que está afeta a esta atividade, torna-se particularmente importante identificar onde reside o titular dos dados, em específico, se na UE e onde está situado o estabelecimento do responsável pelo tratamento de dados pessoais, mesmo que o tratamento ocorra dentro ou fora da UE.

Caso o tratamento ocorra fora da UE, perceber quais são os outros territórios onde é feito o tratamento de dados e perante qualquer uma destas situações, aferir se estão fundamentados formalmente, em suporte documental, os riscos inerentes à gestão, partilha e tratamento de dados pessoais.

O auditor deverá certificar-se de que a empresa possui procedimentos internos capazes de garantir e evidenciar que a recolha e o tratamento dos dados pessoais são concretizados segundo a política de proteção de dados e que todos estes procedimentos, bem como, todos os contratos escritos com clientes, fornecedores, pessoal ou subcontratantes que a Organização executa estão devidamente identificados e suportados.

De igual modo, deve verificar se a entidade possui evidências, em matéria de RGPD, de todas as atividades de recolha e de tratamento de dados, o que efetuou e das quais foi responsável, se identifica todas as organizações externas com as quais realizou atividades de processamento de dados e se exige que estas atuem em concordância com o regulamento e suportem com registos todos os procedimentos concretizados.

Neste contexto, analisando a atividade de AL, é percetível que os dados pessoais dos seus consumidores são indispensáveis, para a prossecução dos contratos de alojamento e outros serviços associados ao turismo, como é o caso dos serviços de aluguer de veículos, seguros de viagem, adesão a campanhas de programas turísticos com roteiros, guias ou experiências gastronómicas.

A realização de uma simples reserva de alojamento não carece de um pedido formal de consentimento para a recolha e tratamento de dados pessoais, desde que respeite somente esse propósito, quer isto dizer que, quando o cliente disponibiliza os seus dados pessoais (nome, morada, número de contribuinte, dados bancários, *et cetera*), estes são, efetivamente, indispensáveis para a realização da reserva e é com base neste propósito que são recolhidos e tratados os dados dos consumidores finais.

Reforça-se que a recolha de dados pessoais é em Portugal, indispensável, para efeitos de faturação, de acordo com o estatuído no Decreto-Lei n.º 197/2012 de 24 de agosto, que exige a recolha destes dados.

Complementarmente, é também por imposição legal, conforme o estatuído no artigo 15.º da Lei n.º 23/2007, de 4 de julho, essencial para o controlo da circulação de cidadãos estrangeiros, o preenchimento dos boletins de alojamento para posterior comunicação ao SEF.

Por outro lado, pode-se dar o caso de ter de existir consentimento, por parte dos clientes, como sucede na obtenção de *vouchers*, através de concursos online, visto que as empresas partilham nas suas redes sociais concursos/sorteios com *vouchers* que incluem uma ou duas noites grátis, num dos alojamentos da Organização.

Contudo e para tal, o participante terá de fornecer um conjunto de dados pessoais e consentir o seu uso e armazenamento para que no futuro, caso seja o contemplado, poder ser informado. Nada impede às organizações de AL de, no momento da confirmação da reserva ou do passatempo, recolher junto dos seus clientes, consentimento complementar para efeitos de publicidade, quer seja através de mensagem telefónica ou por e-mail.

Importa que a auditoria incida, numa fase posterior, na análise e na verificação destes mesmos dados e se estes foram mais tarde empregues para finalidades distintas às que motivaram a sua recolha e para as quais não houve pedido de consentimento adicional, podendo ser, a título de exemplo, a comunicação de novas campanhas promocionais.

Compete ao auditor certificar se a Organização obedece ao princípio da minimização de dados, se cumpre com o direito do titular dos dados de consentimento na recolha e utilização dos dados pessoais para efeitos de publicidade, se tem uma política de privacidade nos seus sites e nos sites para os quais opera, mas também, se nestes apresenta uma notificação de utilização de *Cookies* e o respetivo pedido de consentimento.

De facto, para esta área de negócio revela-se muito importante a utilização de *Cookies*, na medida em que, é através destes que se estabelecem muitas vezes através das pesquisas mais recentes e de modo preciso, o utilizador e as suas preferências, sempre que este acede a uma página web ou uma aplicação, capacitando as organizações em aprimorar a qualidade de navegação e ir de encontro com os gostos e necessidades do consumidor.

Embora os *Cookies* simplifiquem o acesso de navegação do consumidor na *Internet*, segundo Marques (2019, p.229), a utilização de *Cookies* agrava-se perante os *tracking cookies* que designa como «[…] *cookies* de publicidade, que servem para monitorizar o comportamento de navegação do utilizador estabelecer perfis, criar publicidade endereçada, na maioria das vezes com o objetivo final do marketing ou publicidade.».

Nestas circunstâncias, caberá à auditoria analisar se os *websites* utilizados pelas organizações limitam os acessos aos seus clientes mediante a aceitação das suas políticas de *Cookies*, ou seja, averiguar se o cliente somente consegue aceder à página web se aceitar forçosamente *Cookies*, em específico, associado a publicidade. Até porque no âmbito do RGPD, tal situação é considerada imprópria, na medida em que o cliente não tem opção de escolha, indo contra o estatuído no regulamento, nomeadamente, quanto à obtenção de consentimento livre, claro e consciente.

Importa salientar que durante uma auditoria ao RGPD no AL, é importante verificar se na Organização houve lugar ao tratamento de um conjunto de categorias especiais de dados pessoais, que se considerem dados sensíveis, uma vez que, o tratamento deste tipo de dados é proibido, salvo exceções, conforme rege o artigo 9.º do RGP.

É cada vez mais frequente existirem alojamentos locais que oferecem experiências diferenciadas ou de luxo, em que prestam serviços conexos como é o caso dos serviços de saúde e bem-estar, medicina alternativa, SPA ou termas, revelando-se imprescindível requer ao titular dos dados o consentimento de determinados dados sensíveis imprescindíveis para a concretização destes serviços. Ao mencionar dados sensíveis afiguram-se os dados genéticos, a origem racial, a etnia, a orientação sexual, entre outros.

Embora o tratamento de dados sensíveis seja proibido não invalida que estes não possam ser realizados, conforme indica o n.º 2 do artigo 9.º do RGPD, é permitido o tratamento de dados sensíveis em situações específicas para as quais o titular dos dados tenha consentido o tratamento, de modo explícito, para uma ou mais finalidades particulares ou caso o tratamento seja imprescindível para proteger os interesses vitais do titular dos dados ou de outra pessoa singular.

Por exemplo, em serviços como massagens redutoras, tratamentos faciais ou acupuntura, revela-se necessário à Organização ter na sua posse informação sobre se o titular dos dados toma medicação, se faz alergia a algum produto ou se tem alguma doença que possa ser impeditiva para a realização de determinado serviço conexo.

Acrescem também as situações em que o tratamento se revele imprescindível para efeitos de medicina preventiva ou para a execução de determinado trabalho, como é o caso de ter de ser feita uma avaliação à capacidade de trabalho de determinado colaborador ou os dados que terão de ser recolhidos e salvaguardados para feitos de medicina e segurança no trabalho, que é de cumprimento obrigatório nos termos dos artigos 328.º a 332.º e 284.º do Código do Trabalho (CT).

Dada a enorme diversidade de dados pessoais que estão inerentes ao turismo, não só em termos de clientes, como também de funcionários, dado que se trata de um negócio tendencialmente sazonal e por consequência, possui uma enorme rotatividade nos colaboradores que operam nestas empresas de AL, cabe à Organização definir desde o início um conjunto de dados que deverá excluir dos seus formulários de recrutamento, como é o caso da origem racial ou étnica, as opiniões políticas ou as convicções religiosas.

No entanto esta área de negócio apresenta algumas particularidades no que concerne aos dados biométricos, com as assinaturas e impressões digitais, que possibilitam reconhecer de modo claro um indivíduo, no sentido em que se torna, cada vez mais recorrente a utilização destes dados como um procedimento elementar de trabalho.

Tome-se de exemplo as impressões digitais para controlar os tempos efetivos de entrada e saída dos colaboradores nas instalações das organizações, controlo de horas extras ou controlo de turnos. É o caso dos serviços de limpeza dos alojamentos ou de serviços de transporte de hóspedes, controlo dos acessos aos armazéns onde se guardam produtos de limpeza ou mobiliário.

Em complemento, as assinaturas para salvaguardar a entrada e saída dos hóspedes, identificar o colaborador que registou determinado pedido feito pelos hóspedes ou que assegurou uma nova estadia. Indo mais além, será necessária uma clarificação jurisprudencial em determinados casos, para os quais é possível recomendar que, através de certos tipos de dados recolhidos durante uma estadia, é possível reconhecer um hóspede pelas suas preferências ou condições, tendo em ponderação que possa ser uma condição de saúde ou uma restrição alimentar.

No decurso do tratamento dos dados é responsabilidade da empresa comprovar a aplicação e cumprimento do RGPD constatando, inequivocamente, a importância e razoabilidade da conservação e do tratamento dos dados pessoais recolhidos.

Em síntese e de acordo com os pontos em análise, existe efetivamente uma mais-valia para a Organização. São apenas exemplos da complexidade que envolve uma auditoria ao RGPD, no sentido em que se traduz na implementação de novos processos organizacionais, adaptados e padronizados para toda a Organização, abandonando os métodos diferenciados adotados nos distintos departamentos e da eventual necessidade da Organização, caso não esteja obrigada a tal, vir a ter um EPD.

### 4.1.2 Auditoria aos Procedimentos Internos e ao Cumprimento do RGPD

Ao longo dos tempos, as empresas foram implementando políticas que carecem de um olhar cauteloso por parte do auditor, visto que vai avaliar a problemática da conformidade com o regulamento e com a restante legislação em vigor.

A impraticabilidade de controlar e gerir o tratamento e gestão da totalidade dos dados disponibilizados pelos consumidores de AL tornou-se, nos últimos tempos, cada vez mais evidente, assim como, a necessidade constante de implementar normas e procedimentos para fazer face à evolução tecnológica e preservar a segurança, privacidade e confidencialidade dos dados pessoais.

Face às políticas organizacionais importa auditar diversas políticas intrínsecas à grande maioria dos departamentos destas organizações, em específico, o tratamento dos dados pessoais, os acessos aos dados, os riscos, contingências e ameaças, à quantidade e qualidade dos dados, funcionários, entre outros aspetos.

Neste sentido, como já mencionado anteriormente importa ao auditor certificar que os tratamentos estão classificados por categorias, incluindo as de dados especiais, definidos prazos de conservação dos dados e estabelecidas políticas que tenham em consideração a natureza, o âmbito, o contexto e finalidades do tratamento.

Compreender se estão estabelecidas condutas de acesso e níveis de autorização, por departamento e por categoria de dados, se estão definidos mecanismos de monitorização e autodomínio aos acessos aos dados seja com ou sem intervenção humana. Apurar se existe controlo da quantidade de dados, da extensão do tratamento assim como verificar o código de ética, conduta e dos regulamentos internos.

#### *4.2.2.1 A conservação dos dados e o consentimento na sua recolha e tratamento*

Embora sejam inúmeros os procedimentos internos a testar numa auditoria, a conservação de dados e o consentimento do titular dos dados na recolha e tratamento possui, salvaguardando melhor opinião de especial importância.

O período de conservação de dados, deve ser sempre que possível, o tempo exclusivamente necessário para a finalidade para os quais os dados foram recolhidos, isto é, não podem ser armazenados por tempo indeterminado. Sucede que não existe legislado qualquer período de tempo específico ou mandatário para o armazenamento de dados. Importa deste modo que seja o responsável pelo tratamento dos dados a criar um conjunto de critérios que o ajudem a definir um período mínimo.

Além da questão relacionada com o período de conservação, também o motivo e necessidade da recolha, bem como, a finalidade de tratamento deve ser pré-estabelecida, sendo responsabilidade do auditor escrutinar se estas se adequam e de igual modo analisar a questão da existência de medidas de segurança adequadas. Sucintamente, quanto mais tempo os dados estiverem armazenados, maior será o risco de perda, destruição ou até mesmo de fraude.

Através do RGPD é também possível avaliar as circunstâncias de recolha de dados pessoais aceitáveis mediante os consentimentos destes. Existem por isso, por cada direito do titular dos dados um conjunto de obrigações a cumprir associados à conservação e consentimento da recolha de dados.

Segundo o artigo 13.º e seguintes do RGPD, importa à auditoria averiguar se no momento da recolha, o titular tem direito à sua disponibilização um leque de informações sobre a recolha, incluindo todas as disposições legais, a identificação e os contactos do responsável ou da Organização responsável pelo tratamento e armazenamento, as finalidades da recolha, o fundamento jurídico para aquela recolha, os destinatários para quem serão endereçados os dados.

Assim como, quais os processos a efetuar para acesso, retificação, limitação e retirada de consentimento, bem como, todas as demais informações legais necessárias.

Para além do mencionado, cabe à auditoria verificar que o pedido de recolha dos dados foi efetuado de forma explicita, bem como, a permissão para o envio de publicidade apenas foi feita quando consentida pelo titular.

Aferir se existe registo do acesso à informação dos dados pessoais, ainda que tenha sido consentido pelo titular, assim como, os dados que estão a ser tratados. Avaliar se houve circunstâncias em que o responsável pelo tratamento dos dados os limitou mesmo, sem que tenha sido consentido (ou não) pelo titular.

Uma auditoria necessária e mais presente na Organização, quer na verificação da conservação dos dados, quer no consentimento do titular dos dados, revelar-se-á uma mais-valia na medida em que irá testar a conformidade da Organização neste domínio, aferindo também outros procedimentos direta ou indiretamente relacionados.

### 4.1.3 Auditoria ao EPD e aos Contratos com Entidades Subcontratadas

Nem todas as organizações estão obrigadas a nomear um EPD, assim sendo, as que queiram optar por instituir na sua estrutura o cargo do EPD devem recorrer à opinião independente da auditoria para que esta proceda a uma avaliação das aptidões do candidato para o cargo.

Independentemente do EPD pertencer aos quadros internos ou quer seja um prestador de serviços externo, tem de ter inequivocamente competências para o exercício das suas funções, especialmente quando entre as diversas funções que possui, este tem a incumbência de informar e aconselhar a Organização e os seus colaboradores sobre o tratamento de dados pessoais regulado no RGPD e restantes disposições legais.

Cabe ao auditor avaliar se o EPD está a cumprir no âmbito das suas funções às especificidades impostas no artigo 39.º do RGPD, em específico deve fiscalizar se as funções do EPD estão em conformidade com o RGPD e com as demais disposições legais, se este está a prestar aconselhamento nas ações de *Data Protection Impact Assessment* (DPIA) e ainda avaliar se está a estabelecer ações de minimização e mitigação dos riscos, a assegurar o cumprimento dos prazos e estipulações legais em situações de incumprimento ou violação de dados.

Por outro lado, é necessário aferir se a nomeação anteriormente mencionada foi comunicada, assim como, os seus contactos disponibilizados à autoridade de controlo nacional (CNPD). Deve ainda, salvaguardar que estão a ser cumpridos os direitos e obrigações do EPD, particularmente, se este está a ser envolvido em todas as questões da Organização que envolvam assuntos de proteção de dados pessoais, se está a ter apoio por parte do órgão de administração e se lhe estão a ser disponibilizados recursos humanos, financeiros e técnicos necessários para a persecução das suas funções.

No que diz respeito às entidades subcontratadas, o auditor deve em primeiro lugar pedir à Organização o registo de todas as entidades subcontratantes com as quais colabora ou já colaborou, por registo englobam-se informações relativas à localização onde operam, morada, contactos e nome do responsável, bem como, os contratos celebrados com estas entidades.

Averiguar quais os departamentos que supervisionam estas relações, os termos com que é fundamentado a recolha e o tratamento dos dados, se está definido o objeto do tratamento, o período de realização, a finalidade, as categorias de dados a serem tratados e restantes condições contratuais.

O auditor deve ter especial enfoque para as obrigações dos subcontratantes em específico, se estes apenas procedem ao tratamento dos dados mediante indicação do responsável pelo tratamento, se houve por parte dos subcontratantes o cuidado de cumprir com os requisitos de confidencialidade e consentimento, mas também se perante situações de violação de dados estes comunicam de imediato ao responsável tais acontecimentos.

Importa também verificar se as entidades subcontratadas cumprem com os códigos de conduta afetos às suas atividades, se estas estão certificadas e a localização onde foram efetuadas, especialmente, caso tenha sido feita transferência de dados para países estrangeiros ou da UE, ou tenham sido utilizados servidores que se encontram noutros países ou ainda que tenham sido utilizados servidores de terceiros para realizar o tratamento dos dados.

Para além da localização do tratamento, convém verificar se o registo de atividades de tratamento contém os dados dos subcontratantes, do responsável pelo tratamento e do EPD, se o tratamento indica quais as categorias de dados trabalhadas, as técnicas utilizadas e possua documentação que assegure que apenas foram tratados os dados estritamente necessários para a realização da finalidade do tratamento.

Face ao mencionado anteriormente, a auditoria deve avaliar se foi cumprida a obrigatoriedade tanto do responsável com os subcontratantes de adotarem medidas técnicas e organizativas que preservem a segurança e a informação dos dados pessoais com os quais realizaram o tratamento dos dados.

### 4.1.4 Auditoria à Segurança e ao Impacto da Proteção de Dados

Perante o contexto tecnológico que vivemos, é na esfera da segurança da informação e da proteção de dados que o principal foco das organizações deverá incidir.

Embora tenha aumentado o número de estudos e de investigações, que têm intervindo para o alcance de novas descobertas e de novas ferramentas para o desenvolvimento dos SI, a segurança de dados e a avaliação de impacto da proteção de dados são duas áreas que requerem enormes investimentos, quer financeiros, tecnológicos, organizacionais, mas sobretudo humanos.

A segurança da informação é um dos tópicos com especial relevo perante o legislado no RGPD, através dos seus artigos o regulamento alerta para diversas situações que deverão ser tidas em atenção, por forma a salvaguardar os direitos e liberdades dos cidadãos.

Individualmente, elenca nos artigos 16.º a 21.º, os direitos dos titulares de dados e no artigo 25.º aborda a proteção de dados desde a conceção e por defeito. Já no artigo 32.º retrata a segurança do tratamento e no artigo 33.º elege as situações relativas à notificação de violações de dados. E por sua vez, no artigo 35.º expõe as medidas necessárias para uma avaliação de impacto.

Face ao legislado, as organizações não só precisam de sistemas mais seguros, coevos e ajustados para corresponder às obrigações do regulamento, como necessitam de formar todos os intervenientes da Organização e habilitá-los para uma adequada implementação do RGPD e das futuras mutações da legislação nacional e internacional.

#### *4.1.4.1 Segurança dos Dados*

O conceito de segurança dos dados é de facto muito vasto uma vez que, compreende a segurança sob a perspetiva física e tecnológica, onde estão compreendidos um número incalculável de procedimentos, especialmente, quando se trata de dados pessoais.

A segurança dos dados requer um cuidado multidisciplinar, desde o momento de recolha, passando pelo consentimento, tratamento, partilha, armazenamento físico e/ou digital, até à eliminação, por forma a assegurar os direitos e liberdades dos titulares dos dados.

Segundo o artigo 32.º do RGPD, é preciso ter em consideração:

> «[…] as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como, os riscos de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco».

A seguridade de um tratamento de dados tem de ter por base a formulação de processos que assegurem o sigilo e a invulnerabilidade dos sistemas e do tratamento dos dados, assim como, a sua integridade na medida em que a Organização se salvaguarde de eventuais perdas de dados.

Por forma a evitar incidentes e asseverar a segurança da informação que dispõem, é fundamental que, as empresas possuam ferramentas de avaliação e controlo adequadas para determinar a eficácia das medidas que instituíram.

Deste modo o RGPD veio estabelecer às empresas que, mediante os seus responsáveis pelo tratamento ou subcontratantes, apliquem medidas organizacionais capazes de garantir a segurança dos dados pessoais, conforme exemplificado na Figura 4.2.

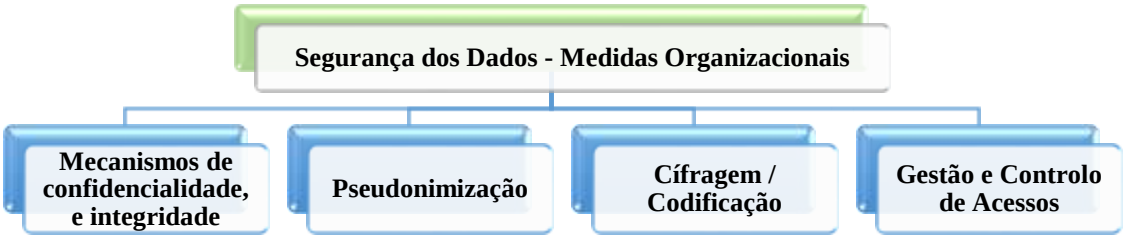



**Figura 4.2 -** Implementação do RGPD no AL

Para além das medidas elencadas pelo regulamento como é o caso da pseudonimização, onde o tratamento de dados pessoais não pode ser atribuído a um titular de dados em específico, do cumprimento do código de conduta e/ou de processos de certificações existem outros procedimentos para atestar a segurança no tratamento de dados.

Especificamente, a avaliação da conformidade com o RGPD, face à globalidade dos processos inerentes às certificações relacionadas com a proteção de dados e dos procedimentos afetos à segurança e TI, comprovados a título de exemplo pelas normas ISO 27001[10] e 27002[11].

Como também a codificação de mecanismos de controlo de acessos, quer físicos quer digitais ou dos próprios dados, que através da segregação de funções, garantam segurança nos acessos, na utilização, partilha e no armazenamento dos dados pessoais.

Adaptando as medidas apresentadas pelo RGPD para o dia a dia das organizações de AL podemos retirar inúmeras propostas de procedimentos a implementar e com os quais a auditoria deverá ter especial atenção para atestar a conformidade das mesmas, nomeadamente, no caso da recolha e tratamento dos dados se a minimização dos dados está a ser cumprida.

Bem como, o princípio da eliminação de dados que não se revelem mandatários para a finalidade do tratamento, por exemplo, num formulário de reserva de um AL será completamente irrelevante as habilitações dos hóspedes, o estado civil, os *hobbies*, contactos de emergência, entre outros.

[10] ISO 27001 é uma norma para sistemas de gestão ao nível da segurança da informação publicado em outubro de 2005 pelo *International Organization for Standardization* e pelo *International Electrotechnical Commission*, com requisitos de certificação e passível de certificação acreditada.

[11] ISO 27002 é uma norma para sistemas de gestão ao nível das tecnologias de informação e técnicas de segurança, sem certificação acreditada

Mesmo perante as informações que se considerem imprescindíveis para a reserva de um AL, estipular prazos para a conservação e manutenção desses dados, ou seja, assim que se atinja as datas pré-estabelecidas possuir métodos informáticos e físicos que eliminem de imediato dos sistemas os dados fornecidos pelos titulares dos dados.

A título de exemplo, preservar os dados dos titulares dos dados até ao último dia da estadia ou até uma semana após o fim da estadia dos mesmos.

Deste modo, sempre que os dados deixem de ser necessários para a finalidade que deu origem à sua recolha são eliminados cumprindo assim as normas do regulamento. Podem também optar pela pseudonimização dos nomes sempre que não se verifiquem ações de publicidade ou de comunicação através de e-mail ou mensagem telefônica e pela codificação dos dados desde o momento da reserva até ao fim da hospedagem.

A análise e avaliação destes procedimentos por parte da Organização não excluem a intervenção da auditoria. Também o auditor tem um papel fundamental na verificação da conformidade dos procedimentos instituídos, que devem englobar um conjunto de regras internas, que contenham princípios de segurança e privacidade.

Sem uma ordem específica a adotar escrupulosamente, uma auditoria de conformidade deve validar a existência ou não de ações de formação à globalidade dos colaboradores e a respetiva regularidade, em especial, no que diz respeito às obrigações e regras associadas à segurança dos dados nos termos da lei.

Verificar se a atribuição das funções e responsabilidades é clara, em matéria de tratamento de dados pessoais e de transferência de dados para terceiros, se estão restringidos os acessos e mecanismos de permissões, quer de instalações como de hardware e software e assegurando que as autorizações de acesso a dados pessoais foram atribuídas apenas às pessoas competentes.

Atestar se existem e se estão bem estabelecidos os processos de automatizações conexos aos acessos de dados via digital, assim como, as medidas de segurança, quer digital como física, mas também analisar se esses mesmos processos e medidas estão a ser testados através de controlos internos.

Embora o RGPD esteja em vigor desde 2018 ainda existem muitas organizações com dificuldade em saber que medidas adotar de modo a atingir um nível de segurança razoável no que concerne aos dados pessoais. Por este motivo importa compreender o RGPD e as atividades particulares de cada Organização.

Visto que o setor do AL é cada vez mais tecnológico e está muitas das vezes dependente das plataformas digitais para divulgar os seus alojamentos, importa ao auditor avaliar a segurança destes, nomeadamente, perceber se foi realizada pela Organização, uma análise minuciosa aos riscos inerentes à utilização dos seus sistemas e aplicações informáticas que sustentam os seus negócios.

O auditor deve dar também especial enfoque à segurança da rede e da base de dados, uma vez que todos os acontecimentos associados à segurança da rede devem estar registados, controlados e avaliados por um sistema de deteção de intrusão. De igual modo, também toda informação sensível armazenada nos SI da Organização, principalmente quando se trate de dados pessoais ou eventualmente dados sensíveis, estes devem estar encriptados conforme estabelecido pelo RGPD e restante legislação.

No caso do setor do AL estas organizações devem elaborar um manual de procedimentos e princípios internos que elenque um conjunto de políticas de segurança e de boa utilização informática para disponibilizarem aos seus colaboradores, que têm um elevado grau de rotatividade devido à sazonalidade que é própria desta atividade.

Também o responsável pelo tratamento de dados deve estabelecer políticas para a correta utilização dos seus sistemas informáticos.

Os colaboradores devem ser um dos principais focos das organizações quando estamos perante a implementação do RGPD. É por isso importante instituir métodos rotineiros nos colaboradores uma vez que, reduz o risco de uma má utilização dos sistemas informáticos e consequentemente, aumenta a segurança dos dados.

Por exemplo, instruir a todos os colaboradores que estes devem, perante circunstâncias de furto ou perda de qualquer equipamento da Organização, que armazene dados pessoais, comunicar de imediato a entidade empregadora.

Ou nos casos em que computador tenha de ser acedido remotamente, para além de acrescer a obrigatoriedade de autenticação através dos dados de registo, palavra-passe ou código pin, quando terminarem o acesso procederem de imediato ao seu encerramento, sendo que os dados de registo e palavras-passes não podem ser guardados para reestabelecer mais tarde outro acesso.

Para além destes então elencados na Figura 4.3 outros exemplos de procedimentos a adotar, de modo a consciencializar todos os colaboradores para uma correta adoção das políticas de proteção de dados dentro da Organização.

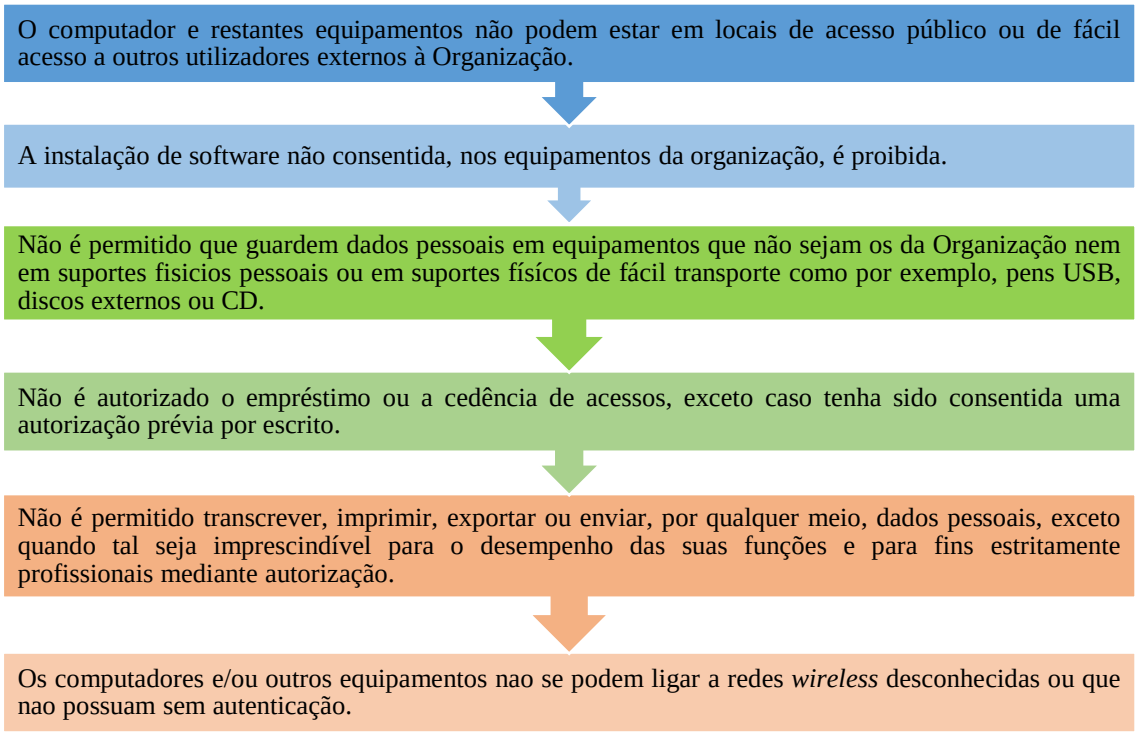



**Figura 4.3 -** Os Colaboradores e os Procedimentos de Segurança a adotar no AL

Por outro lado, compete também à auditoria analisar se as organizações possuem nos seus SI medidas de segurança para a realização do tratamento de dados, validar se foi dado consentimento para a realização do tratamento, quantificar os dados pessoais que podem ser tratados por sistema e se existe controlo sobre esse número.

Enquadrar a extensão do tratamento, verificar se houve cumprimento dos prazos de conservação, atestar os controlos existentes na Organização perante os acessos de dados, quer nos sistemas quer na Organização no registo, modificação e eliminação de dados e se estes estão a ser realizados preservando a segurança da informação, através da realização de testes às medidas técnicas utilizadas.

Para atestar a prossecução da segurança de informação e dos sistemas, o auditor deve proceder a uma análise dos controlos, sempre departamento a departamento, de modo a verificar se dentro de Organização estão instituídas credenciais de acesso, à globalidade dos sistemas informáticos e quem são os responsáveis pela atribuição dessas credenciais.

Por exemplo, verificar qual é o passo dado dentro da Organização quando é eliminado um acesso, se é feito posteriormente a comunicação à direção dos recursos humanos e à direção do departamento da informática.

Ou se para além das credenciais de acesso existe autenticação destes nos SI, quer seja através do nome de utilizador e palavra-passe, código pin ou qualquer outro método de autenticação.

Este tipo de procedimentos deve ser parametrizado antes dos sistemas serem disponibilizados aos colaboradores e para além de parametrizados, devem ser reajustados com alguma regularidade, por exemplo, de dois em dois meses o sistema obrigar os utilizadores a alterarem as suas palavras-passes.

Para além do mencionado, a auditoria deve averiguar se a Organização estabeleceu regras institucionais para a criação da nomenclatura do registo de utilizador, quer dos endereços de correio eletrónico, quer dos registos de computadores ou outros equipamentos, bem como, das palavras-passes. Por exemplo, instituir que a palavra-passe deve englobar letras maiúsculas, minúsculas, números e caracteres especiais.

O auditor deve assegurar que dentro da Organização existe uma política de segurança de informação suportada em formato documental e aprovada pela administração e de igual modo, garantir que estão atribuídas responsabilidades, ao nível da segurança de informação e da privacidade para que, quando os responsáveis atribuam acessos ou perante pedidos de alteração a sistemas informáticos, seja obrigatório que essas atribuições obedeçam a uma autenticação formal.

Importa certificar que para todos os acessos de todos os colaboradores existe um registo em base de dados que permita controlar o horário, a data e os registos acedidos por cada colaborador, bem como, as permissões que foram dadas e quem as autorizou.

Em situações de emergência, no que diz respeito aos centros de processamento de dados, estes devem ter sempre opção de serem suportados por fontes de energia alternativas, para além de que os acessos aos centros de processamento de dados devem ser restritos somente a colaboradores autorizados, o que na maioria das vezes pertencente somente à área de SI.

Todos os equipamentos informáticos devem estar suportados por antivírus, cuja atualização seja feita de modo automatizado.

Como anteriormente mencionado, estes são apenas alguns dos inúmeros procedimentos a adotar e a implementar para assegurar uma boa política de segurança de informação no interior de uma Organização.

No entanto, este é um trabalho que deve ser pormenorizado às especificidades de cada Organização e é um instrumento obrigatório, no sentido em que previne a Organização para situações de incumprimento ou até mesmo de violação de dados pessoais.

Segundo o número 12 do artigo 4.º do RGPD, a violação de dados pessoais consiste na «[…] violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer tipo de tratamento».

Nestes casos, o responsável pelo tratamento está obrigado a notificar a autoridade de controlo competente e o titular dos dados de tal violação. Importa por isso, que a auditoria averigue se, perante o caso de violação de dados, a Organização dispõe de mecanismos tecnológicos capazes de os detetar e se os subcontratantes estão informados da obrigatoriedade de notificar o responsável independentemente de serem ou não responsáveis pela violação dos dados.

É importante também verificar se estão criados procedimentos internos para avaliar a gravidade da violação, bem como, se existem relatórios que suportem cada incidente com toda a informação discriminada. Verificar também se já ocorreram situações destas e se houve comunicação das mesmas à CNPD e ao titular dos dados, se na comunicação foi apresentada a natureza da violação, a categoria de dados envolvidos e o número de dados afetados.

Em suma, inerente à segurança de dados estão afetas inúmeras preocupações e incalculáveis procedimentos a adotar por parte das organizações por forma a tentar mitigar os riscos inerentes à atividade do AL.

É certo que embora o RGPD já vigore há pelo menos dois anos ainda existem muitas organizações no AL com políticas internas debilitadas e pouco eficazes no que diz respeito à proteção de dados.

#### *4.1.4.2 Avaliação de impacto sobre a proteção de dados*

Uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) ou a DPIA ocorre, em conformidade com artigo 35.º, n.º 1 do RGPD, «(q)uando 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».

Precedentemente à realização do tratamento deve ser feita uma AIPD, embora quando se verifique a existência de contingências, que não possam ser minimizadas pelas medidas atuais, os denominados riscos residuais, deverá ser primeiramente consultada a autoridade de controlo, em Portugal é a CNPD.

Este documento (AIPD) deve ser concretizado com regularidade no AL, nos diversos departamentos destas organizações, visto que, esta é uma atividade que opera com uma enorme quantidade de dados em múltiplas segmentações, como é o caso das reservas/vendas online, dos programas de faturação ou dos processos de recrutamento.

Este procedimento, representado na Figura 4.4, tem como propósito pormenorizar o tratamento de dados, estimando a necessidade de realização do mesmo e equacionando a proporção necessidade/risco, com o intuito de apoiar no controlo dos riscos, que possam comprometer os direitos e liberdades das pessoas titulares dos dados pessoais, qualificando-os e estabelecendo medidas eficientes e capazes de mitigar esses riscos.

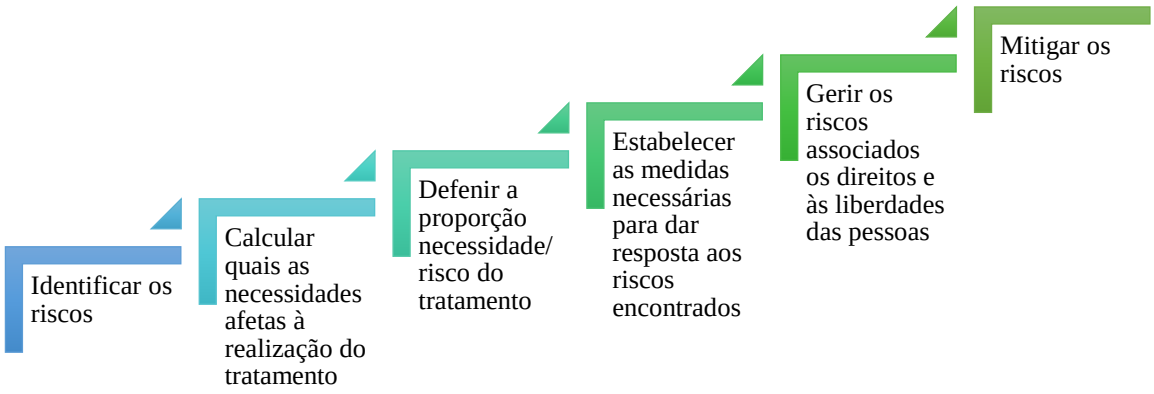



**Figura 4.4-** Processo de Avaliação de Impacto relativo à Proteção de Dados

De modo sucinto a AIPD, para além de estimar os riscos e o impacto das ameaças, determina a probabilidade de ocorrência dos riscos, com o intuito de estabelecer e implementar procedimentos capazes de moderar estes impactos para níveis razoáveis.

Para além do disposto no RGPD, também as autoridades nacionais de proteção de dados, em cooperação com a Autoridade Europeia para a Proteção de Dados (AEPD), disponibilizam umas listas com os casos em que a AIPD é obrigatória.

Embora salvo algumas exceções, estas avaliações não sejam obrigatórias, é imperativo que se ateste um conjunto de verificações para determinar a necessidade de realização de uma avaliação de impacto e posteriormente uma auditoria. A realização destas avaliações, servem de prova aos responsáveis, para certificar a conformidade do tratamento.

A necessidade de realizar uma AIPD deve verificar-se, em específico, nos tratamentos em que o responsável vá recorrer ao uso de novas tecnologias ou soluções inovadoras, de dados sensíveis ou relacionados com condenações penais, em que importa perceber se tal situação conduzirá a circunstâncias que coloquem em causa os direitos e liberdades dos titulares dos dados.

De igual modo, aos tratamentos que imponham uma apreciação contínua e global a aspetos pessoais que estejam fundamentados por tratamento automatizados, incluindo a definição de perfis, que com base nessa apreciação, originem efeitos na esfera jurídica dos titulares ou nos casos em que os tratamentos determinem conjuntos de dados com base em conexões ou interdependências.

A auditoria deve ainda ter em atenção às intervenções de tratamento em grande escala de categorias especiais de dados ou aos casos em que exista controlo constante de zonas acessíveis ao público em grande escala.

Tal como aos tratamentos que derivam de apreciações ou categorizações com base, por exemplo, no desempenho profissional, situação económica ou saúde, que resultem de dados de titulares em condições vulneráveis desde crianças, a doentes ou idosos, ou que limitem os titulares dos dados a exercer direitos ou a contratualizar serviços.

Importa também analisar em que circunstâncias é necessário implementar uma avaliação de impacto. Estas aplicam-se nos casos em que o tratamento tiver como base jurídica o direito da UE ou dos Estados Membros e esse direito regular a operações do tratamento em questão, assim como, nos casos em que já tenha ocorrido anteriormente uma avaliação de impacto sobre a proteção de dados, no âmbito de uma avaliação de impacto geral.

No âmbito das suas funções, a CNPD em concordância com o estatuído no n.º 4 do artigo 35.º, procedeu à divulgação do Regulamento n.º 798/2018 com um conjunto de outras situações em que a realização de AIPD é obrigatória e portanto, deverá ser auditada.

Importa salientar quais as situações de maior risco e que carecem obrigatoriamente de uma avaliação de impacto, conforme exemplificado na Figura 4.5.


**Figura 4.5 -** Casos de AIPD de risco elevado

Posteriormente, compete à auditoria avaliar o cumprimento dos requisitos e deslindar um conjunto de procedimentos que estão afetos a uma DPIA, especialmente se, na avaliação de impacto efetuada foi registada uma explicação fundamentada, no que concerne às operações e finalidades do tratamento, assim como, dos interesses legítimos do responsável pelo tratamento.

Averiguar se no decorrer da AIPD foi feita uma apreciação à necessidade do tratamento, aos danos que este poderia causar para os direitos e liberdades do titular e se foram delineadas soluções, garantias, planos de seguridade e outros métodos capazes de mitigar esses danos e garantir a proteção de dados.

Tendo em conta os objetivos do tratamento o auditor deverá apurar se foi feito um estudo à ponderação adotada na operação, se as medidas executadas estão em conformidade com o RGPD e se foi obedecido o estipulado no código de conduta.

Do mesmo modo que nos casos em que se verifique a existência do cargo de EPD, constatar se o responsável pelo tratamento requisitou um parecer ao mesmo.

Na perspetiva dos titulares dos dados do AL esta avaliação de impacto será imperativa para plataformas globais como é o *Airbnb* ou o *Booking*, pela diversidade e pelos abundantes dados que tratam ou até mesmo quando estes façam, por exemplo, uma seleção dos seus clientes através da consulta de uma base de dados com referência a contas bancárias utilizadas no método de pagamento.

No entanto revela-se importante entender quais serão os principais impactos e fontes de risco para os consumidores de AL, bem como, as principais ameaças que levarão à ocorrência destes riscos e que poderão trazer impactos para os titulares dos dados.

Inicialmente os primeiros impactos que poderão afetar os consumidores de AL passam por que estes recebam e-mails indesejados de marketing e publicidade ou até mesmo de spam, sejam alterados ou eliminados alguns dados das suas contas clientes (data de nascimento, contacto telefónico, etc.), roubo de dados pessoais, ocorram redundâncias em que seja necessário repetir processos ou formalidades, cancelamento das suas reservas ou alteração de dados de reservas como datas ou o número de noites, entre outros.

Estes impactos no AL podem derivar de inúmeras razões desde o uso de discos, *Pen* USB, telemóveis, *tablets*, computadores portáteis desprotegidos, que possam ser conectados a outros dispositivos e através destes apanhar vírus, perda ou roubo destes dispositivos que possam colocar em causa a segurança dos dados dos hóspedes ou a utilização de hardware sensível para uso pessoal.

Assim como, a falta de segurança e restrição de acessos à rede ou a pastas da rede com informação pessoal dos hóspedes, a divulgação involuntária de informação através de conversa telefónica ou via e-mail ou serem vítimas de *Phishing* (roubo informático) ou furto de informação física como é o caso de documentos.

É por isso importante verificar, por exemplo, se:

- Foram estabelecidas normas e políticas de segurança informática e se as mesmas estão de acordo com o RGPD e a restante legislação vigente;
- Estão a ser cumpridos os princípios e direitos dos titulares de dados;
- Existe uma política de monitorização de acessos que aplique uma multiplicidade de ferramentas capazes de evitar a perda de dados devido a falhas no sistema ou a quebras de energia;
- Estão definidos e implementados processos de acesso mediante autenticação seja às instalações, áreas sensíveis ou aos SI, rede, entre outros;
- A comunicação entre os alojamentos e as plataformas digitais ou sites que fazem as reservas é feita através de VPN seguros e a comunicação através de e-mail está encriptada.

A Tabela 4.1 apresenta um conjunto de exemplos de fontes de risco e as possíveis sugestões de recomendações a dar por parte da auditoria com as respetivas medidas de implementação.

**Tabela 4.1 -** Fontes de Risco e Medidas de Mitigação de risco

| Fontes de Risco | Medidas de Mitigação dos riscos |
|---|---|
| • Roubo/ataque informático aos sistemas que possa comprometer ou roubar dados pessoais dos hóspedes.<br>• Instalação de *software* não autorizado ou de origem duvidosa que comprometa a segurança dos dados e dos sistemas de informação.<br>• Erros e vulnerabilidades existentes no *software*.<br>• Não serem feitos ou salvaguardados em fontes externas os *backups*.<br>• Atualizações automáticas de dispositivos eletrónicos. | • Encriptação incluída na rede (VPN).<br>• Criar processos rotineiros para bloquear o acesso a sites com vírus.<br>• Instalação e manutenção de antivírus em todos os dispositivos da organização. E de mecanismos de proteção de *malware* conhecido em base de dados ou desconhecido através de teste de comportamento.<br>• Instituir normas e políticas de segurança informática a aplicar por todos os colaboradores.<br>• Executar com regularidade backups, mesmo que em ambiente de teste, permitindo assegurar que quando necessário estes estão operacionais. |
| • Excesso de rotatividade nos funcionários das organizações, quer seja por má aplicabilidade de políticas internas ou com intencionalidade pode gerar danos operacionais comprometendo informação sigilosa da organização ou até mesmo financeiros dando lugar à extorsão de dinheiro.<br>• Furto ou o extravio de equipamento informático ou de suportes de dados que contém dados pessoais e/ou informação sensível como por exemplo *Pen* USB, computador portátil ou disco externo.<br>• Acesso ilimitado aos servidores e postos de trabalho. | • Deverão ser implementados programas de formação contínua para os colaboradores no âmbito do RGPD.<br>• Acessos restritos e condicionados à rede/ servidor/ base de dados.<br>• Acessos restritos e condicionados, por chefia e departamento, aos espaços físicos onde se encontram armazenados os sistemas de informação e os dados pessoais dos hóspedes em suporte documental.<br>• Implementação e monitorização de ferramentas e processos de gestão de acessos com autenticação.<br>• Colaboradores que tenham acesso aos dados dos clientes deverão possuir uma cláusula de confidencialidade nos seus contratos. |

# 5 Considerações Finais

Nos últimos anos assistimos ao crescimento colossal de novas tecnologias e dos SI. A par destas inovações desenvolveram-se outras áreas de negócio, nomeadamente o turismo, mais especificamente o AL.

Na realidade, o AL veio inovar o processo de expansão das cidades, sobretudo ao nível das capitais europeias, que têm ultrapassado por inúmeros desafios de reabilitação e desenvolvimento urbano para fazer face à procura crescente de turismo. No entanto, não só o crescimento dos SI e das novas tecnologias necessitam de atenção, como também o célere desenvolvimento das plataformas digitais que suportam o turismo.

Ainda que numa primeira instância não se encontre uma ligação entre o AL e a Proteção de Dados, cada vez mais estas temáticas estão interligadas, uma vez que a atividade de AL depende das plataformas digitais para sustentar os seus negócios.

Acresce que, aos SI são disponibilizados um número incalculável de dados pessoais, quer para a efetivação das reservas como para a realização dos pagamentos. É certo que ambas as temáticas têm vindo a sofrer constantes reformas legislativas, muito por causa do aumento da insegurança na partilha de dados pessoais.

Por consequência e em complementaridade com a problemática da privacidade e da proteção de dados, que tem vindo a adquirir especial interesse por parte dos cidadãos, surgiu a necessidade de implementar um regulamento que viesse uniformizar os direitos considerados fundamentais de cada cidadão.

A confiança que outrora vigorava nas antigas regras de proteção de dados estagnou e fez-se sentir na economia. Para tal foi necessário agir perante os distintos contextos de risco existentes na Europa. Por efeito da utilização generalizada e desadequada dos dados pessoais e com o objetivo de instituir procedimentos específicos que salvaguardassem a proteção de dados, a UE publicou no ano de 2016, o RGPD.

Aprovado e em vigor desde maio de 2018, pelo Parlamento Europeu e pelo Conselho Europeu, defende os direitos e as liberdades elementares de indivíduos singulares, sobretudo o direito à proteção dos dados pessoais e estabelece as normas respeitantes à proteção das pessoas singulares, ao nível do tratamento e à livre circulação dos dados.

Perante uma economia fundamentalmente apoiada por SI, torna-se imperioso analisar os métodos adotados, ao nível da proteção de dados pessoais e pelas organizações de AL, evidenciando a necessidade de os auditar.

Com inestimáveis suscetibilidades inseridas nas organizações, revela-se crucial o papel da auditoria e dos auditores, como instrumento de transparência, independência e fiabilidade no apoio e desenvolvimento destas. Não intervém somente ao nível do incentivo no aperfeiçoamento do sistema de controlo interno e por inferência da segurança das recomendações prestadas às administrações das organizações.

A auditoria tem vindo ao longo dos anos a desenvolver-se a par com as necessidades das organizações e a adquirir especial interesse pelas mesmas, no sentido em que apoia a totalidade dos controlos intrínsecos a todos os departamentos existentes numa Organização e a temática da proteção de dados não foi diferente.

Com o RGPD os auditores tiveram de se adaptar às novas exigências e políticas de segurança e proteção de dados passando o intuito de uma auditoria de conformidade ao RGPD por averiguar a exatidão e concordância dos procedimentos internos face às disposições legais.

Alcançar este propósito só é possível através de um conjunto de avaliações pormenorizadas aos diversos componentes que sustentam a conformidade deste regulamento, particularmente, os jurídicos, processuais e tecnológicos.

Com base no mencionado, o intuito basilar deste estudo passou por identificar os principais mecanismos adotados na atividade de AL face ao RGPD, tendo por base um questionário dirigido a organizações que desempenham no ramo do AL, incluído os seus colaboradores, quer internos ou externos e que cumprissem, em simultâneo, dois requisitos: possuem e/ou trabalham em estabelecimento de AL em Portugal; possuem e/ou trabalham com dados pessoais em empresas que prestam serviços para organizações do setor do AL.

A análise apresentada, bem como, as reflexões que se alcançaram encontram-se fundamentadas pelos resultados obtidos, onde são identificadas situações de incumprimento por parte das organizações de AL relativamente à proteção dos dados pessoais e ao estatuído no RGPD.

Deste modo, o pretendido era dar resposta à questão de partida que sustenta o presente estudo "Passados dois anos desde a aprovação do RGPD estarão as organizações de AL a cumprir com os critérios indicados por este regulamento ou necessitarão de apoio por parte da Auditoria?".

Neste contexto, foi em primeira instância verificada a adequabilidade da amostra recolhida, para poderem ser tiradas conclusões, onde foi calculado o número mínimo a extrapolar, com um grau de confiança de 90%. Após extrapolada a amostra foi feita a sua caracterização de modo a retirar o melhor enquadramento possível tendo em conta as respostas obtidas.

Perante uma amostra substancialmente constituída por micro entidades, as conclusões tiveram por base uma análise estatística, onde na primeira parte foi possível tirar ilações sobre o nível de conhecimento das organizações e dos seus colaboradores no que diz respeito ao conceito do RGPD, se estas estavam familiarizadas com os objetivos da Organização face à política de proteção de dados, compreender se existiam processos organizacionais associados à segurança dos dados, qual o nível de preparação tecnológica e quais as áreas que consideravam necessitar de maior reestruturação para corresponder aos desafios impostos pelo RGPD.

No decorrer da análise aos resultados obtidos foi possível depreender que a maioria dos inquiridos, concordam que as empresas para as quais trabalham possuem conhecimento sobre o RGPD, no entanto quando questionados sobre os objetivos da Organização e se estes estão em concordância com a política de proteção de dados, surgiram as primeiras incertezas.

Na primeira fase do questionário foi possível compreender que embora o RGPD esteja em vigor há já pelo menos dois anos, as organizações ainda não estão preparadas para cumprir com os requisitos impostos no regulamento.

Pese embora a grande maioria destas organizações sejam micro entidades, o facto é que por esta razão, poder existir uma capacidade diminuta na implementação de procedimentos e políticas internas, a maioria dos inquiridos discordou com o facto de existirem implementadas na Organização, políticas relativas à proteção de dados.

Perante esta realidade, permite identificar que a amostra em estudo requer uma auditoria pormenorizada, onde seja feito o enquadramento dos procedimentos atualmente adotados face às normas em vigor, recomendar especializações e certificados onde as organizações adotem ou garantam, em parte, procedimentos de acordo com a conformidade exigida e com o RGPD.

Esta evidência factual, permitiu justificar a elaboração e enumeração de alguns dos principais contributos para a monitorização e realização de Auditorias ao RGPD nas entidades de AL.

Apenas mediante a realização de uma avaliação de conformidade com o RGPD, será idealmente possível avaliar o nível de capacitação tecnológica de uma Organização.

Ainda assim, foi inquirida à amostra uma opinião mais específica, onde uma maioria significativa das pessoas afirmou que considera que a tecnologia que existe atualmente nas suas organizações não satisfaz parcialmente os requisitos do RGPD.

Na verdade o RGPD não elenca medidas técnicas específicas para a adequabilidade e conformidade do regulamento, quer isto dizer que, compete às organizações investigarem e determinarem qual o nível de adequação que dispõem e quais as opções e soluções necessárias a implementar.

A existência de procedimentos e políticas não é, por si só, fator que habilite uma Organização de estar em conformidade com o RGPD. De acordo com a amostra, quando questionados se os procedimentos atualmente adotados na Organização para a qual trabalham satisfazem os requisitos do RGPD, mais uma vez a maioria discordou.

O que permite concluir que para além de existir um défice no que diz respeito às noções elementares do RGPD, as organizações não estão a adotar políticas internas suficientes para cumprir com o estipulado no regulamento.

Em seguida, numa segunda parte do inquérito foi observado o nível de conhecimento das organizações face ao EPD onde, em semelhança à questão sobre a noção do conceito do RGPD, a maioria alegou ter conhecimentos sobre o tema.

No entanto quando questionados sobre a posição, funções e responsabilidades do EPD e sobre a existência de ter dentro da Organização alguém designado para o cargo, a maioria afirmou desconhecer. O que permitiu também depreender que a generalidade dos inquiridos desconhecia profundamente as situações em que o EPD deverá estar envolvido e se este atua em conformidade com o regulamento.

Para finalizar esta parte do inquérito, foi colocado à disposição dos inquiridos seis opções conexas a procedimentos internos, especialmente relevantes, para a implementação do RGPD numa Organização, com o desígnio de assinalarem qual a opção que consideram precisar de maior intervenção ou, possivelmente, até de ter de instituir dentro da Organização.

Destacaram-se a formação relativa à proteção de dados para os colaboradores e a adequação das políticas internas concordantes com o RGPD.

A adequação das políticas internas e de igual modo a formação são áreas chave para uma boa implementação do RGPD, uma vez que acabam por ser processos de conformidade extremamente importantes para assegurar a política de privacidade e proteção de dados.

As ações de formação serão sempre essenciais no cumprimento do RGPD, na medida em que irão sempre existir novas disposições legais, medidas de controlo ou até mesmo decisões judiciais. Por sua vez, a validação aos acessos foi uma das opções com menos respostas o que revela por si só falta de conhecimento sobre o tema.

A gestão de acessos deve ser tida em consideração de forma rigorosa e criteriosa, visto que dentro da Organização é fundamental que exista uma base estrutural de cargos hierárquicos, capaz de segregar funções e acessos por forma a preservar a privacidade e segurança dos dados, assim como, os princípios da minimização e limitação de dados.

Muitas vezes quando se fala em gestão de acessos, as organizações tendem a pensar nos acessos físicos, no entanto os digitais são cada vez mais importantes. Sobretudo porque carecem de ferramentas e recursos, como é o caso de palavras-passe, antivírus e backups capazes de salvaguardar a informação, assim como, de garantir que é feito um controlo sistemático aos acessos, possibilitando prevenir futuras situações de roubo de informação.

Atualmente a complexidade das empresas, independentemente da sua dimensão, obriga a que seja instituído um conjunto de ferramentas para que, de forma estruturada e clara, todos os intervenientes estejam em sintonia, que saibam quais as suas funções e os procedimentos internos da Organização por forma a conseguir compreender se os mesmos estão em conformidade com o RGPD e com a política de proteção de dados.

No entanto no que concerne às respostas obtidas, relativamente ao registo e tratamento de dados, em seguimento das conclusões que já tinham sido retiradas nos dois capítulos anteriores, também neste foi possível retirar que existe uma enorme escassez de procedimentos implementados por parte das pequenas organizações.

Embora os inquiridos afirmem que os procedimentos estão pontualmente de acordo com o RGPD e que apenas são necessárias pequenas correções aos processos já existentes, os próprios afirmam que as organizações não estão capazes de gerir os acessos aos dados pessoais dos seus hóspedes. De acordo com as respostas obtidas é possível perceber que tal circunstância coloca em causa a segurança da informação e por efeito, a imposição base assente no regulamento.

Perante outras questões foi notória a percentagem significativa de respostas para as quais os inquiridos não tinham opinião, o que leva a retirar duas hipóteses de conclusão ou as questões foram mal formuladas e por efeito as respostas disponibilizadas confundiram os respondentes, ou que existe um claro desconhecimento sobre o tema.

Importa salientar que face às respostas obtidas no inquérito é evidente que existe uma grande incerteza na avaliação da possibilidade de serem aplicadas ou não penalizações, sobretudo devido à imprecisão existente sobre alguns aspetos referentes ao regulamento, nomeadamente, no que diz respeito à implementação e adequabilidade dos procedimentos internos e à segurança dos dados. É pertinente verificar que ao longo da dissertação foi possível analisar, estudar e sintetizar alguns dos aspetos essenciais presentes no RGPD, mais especificamente, a proteção de dados pessoais de pessoas singulares no AL.

A verificação e análise das políticas corporativas, referentes ao registo e tratamento de dados pessoais, que existem numa empresa, é um dos pontos mais cruciais do plano de trabalho de uma auditoria, na medida em que permite aferir o nível de conformidade de uma Organização com o regulamento. Visto que a atividade de AL é uma área que está afeta a uma diversidade enorme de recolha e tratamento de dados, acresce a importância de serem realizadas auditorias de conformidade a este setor, sendo feitas análises às áreas mais deficitárias em termos de medidas adotadas pela Organização e pelo responsável pelo seu tratamento.

Mediante os procedimentos adotados e sustentados por um planeamento completo e estruturado, é necessário analisar as componentes que sustentam o atual regulamento de proteção de dados para posteriormente as personalizar e adaptar às necessidades do AL.

No âmbito da componente jurídica, deve ser feita uma avaliação à licitude do tratamento de dados, à salvaguarda dos princípios e direitos dos titulares dos dados, à adequação contratual do encarregado de proteção de dados e demais entidades subcontratadas e sobretudo, assegurar o cumprimento do regulamento.

Posteriormente com base na análise aos componentes processuais, detalhar processos como a identificação, recolha, partilha, processamento e armazenamento de dados pessoais, elucidar a importância dos códigos de conduta, manuais de procedimentos e políticas internas, mas também manuais de apoio a processos relacionados com o tratamento de dados pessoais.

Alertar sobre a relevância da avaliação de impacto de dados pessoais, assim como, da segurança da informação dos dados, a necessidade de notificação perante casos de violação de dados e a identificação e atribuição inequívoca de responsabilidades.

A auditoria ao AL tem como um dos principais riscos a insegurança dos sistemas, onde fontes externas são capazes de recolher dados sensíveis ou sigilosos das organizações e dos consumidores. Não é possível assegurar uma segurança completa aos sistemas de reservas de AL. No entanto existem procedimentos de controlo capazes de diminuir este risco.

Associada à proteção da confidencialidade, plenitude e disponibilidade das informações sensíveis das organizações e consequentemente dos seus consumidores, conduz-nos à necessidade de adaptação do RGPD por parte das empresas nas suas estruturas informáticas ao nível de diversas temáticas. Por exemplo, através de políticas de segurança com palavras-passes, antivírus, registos de acesso, segurança nas bases de dados e software de modo a garantir nas políticas internas conformidade com o RGPD.

Elencados os principais pontos detetados com base nos resultados obtidos ao logo do estudo e pese embora a generalidade destas entidades se caracterizem, como micro ou pequenas empresas e ainda que não estejam obrigadas a auditoria externa e a algumas das especificidades estatuídas no RGPD não é possível descredibilizar os enormes volumes de dados pessoais que operam diariamente, nem os riscos que daí ocorrem e interferem com a vida privada dos consumidores. Numa era em que a auditoria interna tem desenvolvido um papel cada vez mais presente e desafiante no dia-a-dia das organizações, é espectável que lhe seja exigida uma nova abordagem no que concerne à proteção de dados pessoais.

Pretendeu-se por este motivo destacar o interesse e o papel dos auditores, bem como, a necessidade de atuação da auditoria perante a problemática do RGPD no AL, através de mecanismos de controlo que poderão ser capazes de mitigar esta lacuna existente na aplicabilidade e no cumprimento deste regulamento.

A realização da presente dissertação permitiu determinar que a aplicabilidade da legislação vigente revela-se insuficiente, tendo em consideração que a obrigatoriedade da auditoria se restringe às designadas grandes empresas e a do EPD, somente se aplica às organizações que reúnam os requisitos estipulados no RGPD.

Neste sentido, consciente do que ficou por abordar e aprofundar deixa-se em aberto para investigações futuras, a problemática da aplicabilidade da atual legislação no que diz respeito à proteção de dados pessoais face às micro e pequenas empresas de AL no que respeita ao âmbito, suficiência e necessidade tendo em consideração os riscos elevados que este setor possui.

Estudos futuros poderão perspetivar ainda o desenvolvimento de um projeto capaz de implementar uma ferramenta competente e eficaz de auditar não só as plataformas de AL como o processamento e partilha dos dados pessoais dos consumidores.

E por último, analisar a situação financeira das empresas de AL e o impacto económico sentido em Portugal, após a pandemia provocada pela Covid-19. Esta pandemia, assim como os impactos gravíssimos que causará à economia e em especial ao AL, é um tema extremamente pertinente para futuros projetos de investigação.

As limitações da presente investigação possuem naturezas distintas das quais se destacam, a ausência de informação sistematizada sobre a política de proteção de dados no setor do AL, os procedimentos a adotar por estas organizações, tendo em conta o estatuído pelo RGPD e a reduzida adesão por parte das organizações contactadas para a resposta ao questionário que dificultou a recolha de informação adicional.

A possibilidade de colmatar esta limitação, assenta no número de respostas obtidas e estender a estudos futuros com uma amostra mais alargada, novas recomendações de procedimentos de apoio à implementação do RGPD e possíveis controlos de auditoria mediante os procedimentos implementados.

## Referências Bibliográficas


AAA. (1973). Studies in Accounting Research: A statement of basic auditing concepts. New York: American Accounting Association

Antunes, M., & Rodrigues, B. (2018). Introdução à Cibersegurança. Lisboa: FCA.

Arens, A. A., Randal, J. E., & Beasley, M. S. (2003). Auditing and Assurance Services - An Integrated Approach (Ninth Edition). New Jersey: Prentice Hall.

AHRESP - Associação da Hotelaria, Restauração e Similares de Portugal. (2020). Manual Prático do RGPD para o canal Horeca. [Consulta 20 setembro 2020]. Disponível: https://ahresp.com/app/uploads/2020/02/AHRESP_Manual-de-boas-praticas_fev2020.pdf

Avison, D. E., & Myers, M. D. (1995). Information systems and anthropology: An anthropological perspective on IT and organizational culture. Information Technology & People, 8(3), 43–56.

Balcão Único Eletrónico. [Consult. 23 maio 2020]. Disponível em: https://eportugal.gov.pt/empresas/services/balcaodoempreendedor/Licenca.aspx?CodLicenca=2637

Barreiro, M. (2007). Auditoria Interna – Aliada da estratégia empresarial. Revista de Auditoria Interna, nº 27, abril /julho. [Consult. 23 março 2020].

Brauckmann, S. 2017. City tourism and the sharing economy–potential effects of online peer-to-peer marketplaces on urban property markets. Journal of Tourism Futures, 3(2): 114-126.

Buckingham, R. A., Hirschheim, R. A., Land, F. F., & Tully, C. J. (Eds). (1987). Information systems education: Recommendations and implementation. Cambridge: Cambridge University Press.

Canotilho, J. G. & Moreira, V. (2014). Constituição da República Portuguesa Anotada. Vol. I. Coimbra Editora.

Castro, C. S. (2005). Direito da Informática, Privacidade e Dados Pessoais. Almedina.

Chambers, R. J. (1995). An Accounting Thesaurus: 500 Years of Accounting. Pergamon.

CNPD. Espaço RGPD. Comissão Nacional de Proteção de Dados. [Consulta em 16 janeiro 2020] – https://www.cnpd.pt/bin/rgpd/rgpd.htm

Código Civil Portuguez de 1867. [Consulta em 15 janeiro 2020]. Disponível em: http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Codigo-Civil-Portugues-de-1867.pdf

Costa, C. B. (2017). Auditoria financeira – teoria & prática. 11.ª edição. Lisboa: Rei dos livros.

Couto, M. L. (2016). O E-Commerce à luz do direito – Análise do Regulamento Geral da Proteção de Dados – A Uniformização na União Europeia. Dissertação de Mestrado apresentada à Faculdade de Direito do Porto - UCP.

Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008. [Consulta em 22 novembro 2019]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008F0977&from=PT

Diário do Governo, Decreto n.º 41035, de 20 de março de 1957. [Consulta em 9 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/653691

Diário da República, Lei n.º 10/91, n.º 98/1991, Série I-A de 1991-04-29. [Consulta em 8 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/599769

Diário da República, Decreto-Lei n.º 7/1991, Série I-A de 1991-01-09. [Consulta em 10 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/693442

Diário da República, Decreto-Lei n.º 167/1997, n.º 152/1997, Série I-A de 1997-07-04. [Consulta em 9 novembro 2019]. Disponível em:

https://dre.pt/application/conteudo/156001

Diário da República, Decreto-Lei n.º 152/1997, Série I-A de 1997-07-04. [Consulta em 9 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/156001

Diário da República, Lei n.º 67/98, n.º 247/1998, Série I-A de 1998-10-26. [Consulta em 8 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/239857

Diário da República, Lei n.º 43/2004, n.º 194/2004, Série I-A de 2004-08-18. [Consulta em 8 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/480712

Diário da República, Lei n.º 23/2007, n.º 127/2007, Série I de 2007-07-04. [Consulta em 12 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/635814

Diário da República, Decreto-Lei n.º 39/2008, Série I de 2008-03-07. [Consulta em 10 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/247248

Diário da República, Decreto-Lei n.º 197/2012, n.º 164/2012, Série I de 2012-08-24. [Consulta 8 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/174548

Diário da República, Lei n.º 2/2014, n.º 11/2014, Série I de 2014-01-16. [Consulta em 12 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/571007

Diário da República, Decreto-Lei n.º 128/2014, Série I de 2014-08-29. [Consulta em 7 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/56384880

Diário da República, Decreto-Lei n.º 63/2015, n.º 79/2015, Série I de 2015-04-23. [Consulta em 7 novembro 2019]. Disponível em:

https://dre.pt/application/conteudo/67059141

Diário da República, Lei n.º 62/2018, n.º 161/2018, Série I de 2018-08-22. [Consulta em 11 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/116152179

Diário da República, Lei n.º 58/2019, n.º 151/2019, Série I de 2019-08-08. [Consulta 11 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/123815982

Diário da República, Lei n.º 59/2019, n.º 151/2019, Série I de 2019-08-08. [Consulta 11 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/123815983

Diário da República, Portaria n.º 217/2020, Série I de 2020-11-06. [Consulta 6 novembro 2020]. Disponível em: https://dre.pt/application/conteudo/147814581

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. [Consulta 22 novembro 2019]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. [Consulta 22 novembro 2019]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT

Ecommerce Europe & EuroCommerce. (2018). The European Ecommerce Report 2018: relevant findings outlined. Disponível em:

https://www.retailinsiders.nl/docs/77f3cdc4-38b2-4dd2-8938-cb4293cc8c19.pdf

Estratégia Turismo 2027. [Consulta em 20 setembro 2020]. Disponível em: https://estrategia.turismodeportugal.pt/sites/default/files/Estrategia_Turismo_Portugal_ET27.pdf

Europeia, C. (s.d.). Orientações sobre os encarregados da proteção de dados (EPD). [Consulta 20 setembro 2019]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection_pt

Europeia, C. (s.d.). Regras da EU em matéria de proteção de dados. [Consulta em 20 setembro 2019]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_pt

EY & AM&A. (2017). Avanço da Economia Digital em Portugal. [Consulta 20 setembro 2020].Disponível:https://ind.millenniumbcp.pt/pt/negocios/financiamento/Documents/BCP_Economia-Digital-Relatorio-Final-201710.pdf

Fazendeiro, A. (2017). Regulamento Geral sobre a Proteção de Dados. Coimbra. Almedina.

Fazendeiro, A. (2018). Regulamento Geral de Proteção de Dados. Coimbra: Almedina.

Garcia, M. O. 2017. Arrendamento de curta duração a turistas: Um (impropriamente) denominado contrato de alojamento local. Revista Eletrónica de Direito, 3.

Gomes, A. (11 de Março de 2019). Alojamento local ou arrendamento tradicional: qual o mais rentável?. DECO Proteste. [Consulta 9 junho 2019]. Disponível em: https:// www.deco.proteste.pt/investe/investimentos/imobiliario/comprar-casa/ analises/2019/03/alojamento-local-arrendamento-tradicional-rentavel

Guimarães, F. & Pereira, M. L. (2018). Regulamento Geral de Proteção de Dados: Manual prático. Porto: Vida Económica.

Gurran, N. (2017). Global Home-Sharing, Local Communities and the Airbnb Debate: A Planning Research Agenda. Planning Theory and Practice, 9357, 1–7. doi:10.1080/14649357.2017.1383731

Gurran, N., & Phibbs, P. (2017). When Tourists Move In: How Should Urban Planners Respond to Airbnb? Journal of the American Planning Association, 83(1), 80–92. doi:10.1080/01944363.2016.1249011

Gutiérrez, J., García-Palomares, J. C., Romanillos, G., & Salas-Olmedo, M. H. 2017. The eruption of Airbnb in tourist cities: Comparing spatial patterns of hotels and peer-to-peer accommodation in Barcelona. Tourism Management, 62: 278-291.

Holmes, A. W. (1956). Auditing principles and procedure. 4.ª edição. Homewood.

IIA - The Institute of Internal Auditors. The Institute of Internal Auditors – Definition of Internal Auditing. [Consulta 9 junho 2019]. Disponível em: https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of Internal-Auditing.aspx

Instituto Nacional de Estatística. [Consulta 29 agosto 2019]. Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=458718662&DESTAQUESmodo=2

Lajoso, P. G. (2005). A importância da Auditoria Interna para a Gestão de Topo.

Lisboa. Revista de Auditoria Interna, Nº 19, p. 10-12. [Consulta em 20 junho 2020]

Mamede, H. S. (2015). Revista de Ciências da Computação, nº10. Notas leitura / Recensão crítica [de] Protection of Personal Data, p. 91 a 98.

Marques, M. M. (2019). O Regulamento Geral sobre a Proteção de Dados. Librum Editora.

Ministério Público - Procuradoria-Geral Distrital de Lisboa: Lei da Proteção de Dados Pessoais [Consulta em 10 junho 2019]:

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=156&tabela=leis&so_miolo

Morais, G. & Martins, I. (2013). Auditoria Interna - Função e Processo (4ª Edição).

Munkøe, M. M. (2017). Regulating the European Sharing Economy: State of Play and Challenges. Intereconomics, 52(1), 38–44. doi:10.1007/ s10272-017-0641-3

Neto, R. (4 de Abril de 2020). Da caça de hóspedes nas redes sociais aos saldos no Airbnb. Alojamento Local desesperado com o Covid-19. ECO. [Consulta em 8 julho 2020]. Disponível em: https://eco.sapo.pt/2020/04/04/da-caca-de-hospedesnas-redes-sociais-aos-saldos-no-airbnb-alojamento-local-desesperado-com-ocovid-19/

Oliveira, J. A. (2006). Método de Auditoria a Sistemas de Informação. Porto: Porto Editora.

Patrício, M. (2016). Direito do Turismo e Alojamento Turístico. Coimbra: Almedina

Parlamento Europeu e do Conselho. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho publicado em 27 de abril de 2016. Regulamento Geral de Proteção de Dados. [Consulta em 20 novembro 2019]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

Pinheiro, A. S. (Coord.) (2018). Comentário ao Regulamento Geral de Proteção de Dados. Coimbra: Almedina.

Pinheiro, J. L. (2014). Auditoria Interna - Manual Prático para Auditores Internos (3ª Edição). Editora Rei dos Livros.

Pires, R. C. (2011). Tributação Internacional do Rendimento Empresarial gerado através do Comércio Eletrónico. Coimbra: Almedina.

Portal do Cidadão. A CNPD. [Consulta em 20 maio 2020]. Disponível em https://www.portaldocidadao.pt/web/comissao-nacional-de-protecao-de-dados/comissao-nacional-de-protecao-de-dados

Quivy, R. & Campenhoudt, L. (1998). Manual de Investigação em Ciências Sociais. 2.ª edição Lisboa: Gradiva.

Quivy, R. & Campenhoudt, L. (2005). Manual de Investigação em Ciências Sociais. 4.ª edição Lisboa: Gradiva.

Registo Nacional de Turismo. [Consulta 20 maio 2020]. Disponível em: https://registos.turismodeportugal.pt/HomePage.aspx

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016). [Consulta março, abril e maio 2020]. Jornal Oficial da União Europeia.

Rubio, A., Silva, J. & Guimarães, T. (2014). Auditoria Interna e sua Importância para as Organizações. Revista Saberes da FAPAN (2.ª Edição). Dezembro 2014. [Consulta 20 novembro 2019]. Disponível em: http://fapan.edu.br/media/files/2/2_118.pdf

Sá Soares, F. (2010). Sebenta de Auditoria de Sistemas de Informação. Universidade do Minho.

Saldanha, N. (2018). Novo Regulamento Geral de Proteção de Dados. Lisboa: FCA.

Saldanha, N. (2019). RGPD Guia prático para uma auditoria de conformidade. Lisboa: FCA.

Sarmento, M. (2013). Metodologia Científica para a elaboração, escrita e apresentação de teses. Lisboa: Universidade Lusíada Editora.

Seixas, J. (2019). Área Metropolitana de Lisboa. In J. A. R. Fernandes, L. Carvalho, P. Chamusca, & T. Mendes (Eds.), A Airbnb em Portugal. Porto: Book Cover Editora.

Sousa, José M. e Baptista, Sales C. (2011). Como fazer Investigação Dissertações, Teses e Relatórios Segundo Bolonha (1ª Edição). Lisboa: Pactor.

Taborda, D. (2015). Auditoria - Revisão Legal das Contas e Outras Funções do Revisor Oficial de Contas (2ª Edição). Lisboa: Edições Sílabo.

Teixeira, M. (2006), O contributo da Auditoria Interna para uma Gestão eficaz, Dissertação de Mestrado em Contabilidade e Auditoria.

The Travel & Tourism Competitiveness Index 2019 do World Economic Forum. [Consulta 20 abril 2020]. Disponível em: https://www.weforum.org/reports/the-travel-tourism-competitiveness-report-2019

Turismo de Portugal. [Consulta julho e agosto 2020]. Disponível em: https://registos.turismodeportugal.pt/HomePage.aspx

Zeferino, A. (2016). Digital Marketing Analytics. Sabedoria Alternativa Edições.

Yáñez, S. (2016). Reclamar o «Direito ao esquecimento». JusJornal, N.º 2509. Wolters Kluwer. [Consult. 18,19 e 20 maio 2020]

Weber, A. R. (1999). Information Systems Control and Audit. 1.ª Edição. Prentice Hall.

## Apêndice 1: Caracterização da amostra por atividade em função da faixa etária e dispersão geográfica

| **Alojamento Local** | **78** | **Serviços de Consultoria** | | | | | | **Gestão Hoteleira** | **19** |
|---|---|---|---|---|---|---|---|---|---|
| | | **Consultoria e Gestão de Projetos** | **3** | **Auditoria** | **4** | **Contabilidade** | **6** | | |
| **< 25 a 35 Anos** | **9** | **< 25 a 35 Anos** | **3** | **< 25 a 35 Anos** | **1** | **< 25 a 35 Anos** | **5** | **< 25 a 35 Anos** | **4** |
| Arquipélagos | 2 | Arquipélagos | - | Arquipélagos | - | Arquipélagos | 1 | Arquipélagos | - |
| Centro | 6 | Centro | 2 | Centro | 1 | Centro | 3 | Centro | 3 |
| Norte | 1 | Norte | - | Norte | - | Norte | - | Norte | - |
| Sul | - | Sul | 1 | Sul | - | Sul | 1 | Sul | 1 |
| **≥ 35 a 45 Anos** | **36** | **≥ 35 a 45 Anos** | **0** | **≥ 35 a 45 Anos** | **1** | **≥ 35 a 45 Anos** | **0** | **≥ 35 a 45 Anos** | **7** |
| Arquipélagos | 11 | Arquipélagos | - | Arquipélagos | - | Arquipélagos | - | Arquipélagos | 1 |
| Centro | 6 | Centro | - | Centro | 1 | Centro | - | Centro | 3 |
| Norte | 14 | Norte | - | Norte | - | Norte | - | Norte | - |
| Sul | 5 | Sul | - | Sul | - | Sul | - | Sul | 3 |
| **≥ 45 a 55 Anos** | **17** | **≥ 45 a 55 Anos** | **0** | **≥ 45 a 55 Anos** | **2** | **≥ 45 a 55 Anos** | **1** | **≥ 45 a 55 Anos** | **6** |
| Arquipélagos | 2 | Arquipélagos | - | Arquipélagos | - | Arquipélagos | - | Arquipélagos | 1 |
| Centro | 2 | Centro | - | Centro | 2 | Centro | - | Centro | 1 |
| Norte | 5 | Norte | - | Norte | - | Norte | - | Norte | 2 |
| Sul | 8 | Sul | - | Sul | - | Sul | 1 | Sul | 2 |
| **> 55 Anos** | **16** | **> 55 Anos** | **0** | **> 55 Anos** | **0** | **> 55 Anos** | **0** | > 55 Anos | **2** |
| Arquipélagos | 6 | Arquipélagos | - | Arquipélagos | - | Arquipélagos | - | Arquipélagos | 1 |
| Centro | 4 | Centro | - | Centro | - | Centro | - | Centro | - |
| Norte | 3 | Norte | - | Norte | - | Norte | - | Norte | - |
| Sul | 3 | Sul | - | Sul | - | Sul | - | Sul | 1 |

## Apêndice 2: Questionário

# A Auditoria e a Proteção de Dados dos Consumidores de Alojamento Local

O presente questionário surge de um processo de investigação científica, no âmbito do Mestrado em Auditoria do ISCAL, num projeto de dissertação com o tema: «A Auditoria e a Proteção de Dados dos Consumidores de Alojamento Local»

Pretende-se efetuar um levantamento de controlos de auditoria no que concerne à fiabilidade do tratamento e gestão de dados dos consumidores de Alojamento Local, no âmbito da implementação do Regulamento Geral de Proteção de Dados (RGPD).

Deste modo, o questionário tem por base a perspetiva de profissionais que lidem diariamente com o tratamento de dados pessoais por forma a identificar quais os pontos fortes e os pontos fracos inerentes à atividade do Alojamento Local.

A sua colaboração é essencial e totalmente confidencial.

Obrigada.

E-mail *

A sua resposta

*Obrigatório

## Dados Pessoais

Grupo etário ? *

- < 25 a 35 Anos
- ≥ 35 a 45 Anos
- ≥ 45 a 55 Anos
- > 55 Anos

Dispersão Geográfica *

- Norte
- Centro
- Sul
- Arquipélagos

Em que área de negócio se insere a sua Organização? *

A sua resposta

Qual a dimensão da Organização? *

- Micro Entidade
- Pequena Empresa
- Média Empresa
- Grande Empresa

## Contexto da proteção de dados na organização

Neste capítulo deverá avaliar o nível de conhecimento da Organização onde trabalha no que diz respeito à implementação e aplicabilidade do RGPD.

A sua Organização tem conhecimento do novo Regulamento Geral de Proteção de Dados (RGPD) aprovado pelo Parlamento Europeu? *

- Concordo totalmente
- Concordo em parte
- Não concordo nem discordo
- Discordo em parte
- Discordo totalmente

Está familiarizado com os objetivos da Organização relativamente à política de proteção de dados? *

- Concordo totalmente
- Concordo em parte
- Não concordo nem discordo
- Discordo em parte
- Discordo totalmente

Existem políticas e procedimentos relativos à proteção de dados dentro da Organização? *

- Concordo totalmente
- Concordo em parte
- Não concordo nem discordo
- Discordo em parte
- Discordo totalmente

Considera que a sua Organização está tecnologicamente preparada para o RGPD? *

- Concordo totalmente
- Concordo em parte
- Não concordo nem discordo
- Discordo em parte
- Discordo totalmente

Concorda que os procedimentos atuais da sua Organização satisfazem os requisitos do RGPD? *

- Concordo totalmente
- Concordo em parte
- Não concordo nem discordo
- Discordo em parte
- Discordo totalmente

Na sua opinião quais os departamentos dentro da Organização que considera necessitarem de rever os procedimentos adotados? *

A sua resposta

## Encarregado de Proteção de Dados

Neste capítulo deverá avaliar o nível de conhecimento da Organização onde trabalha no que diz respeito ao Encarregado de Proteção de Dados (EPD).

Tem noção do conceito de Encarregado de Proteção de Dados (EPD)? *

- Conheço totalmente
- Conheço em parte
- Não conheço nem desconheço
- Desconheço em parte
- Desconheço totalmente

Tem conhecimento de na cultura organizacional existir uma definição relativamente à posição, função e responsabilidades que deverão ser atribuídas a um EPD? *

- Conheço totalmente
- Conheço em parte
- Não conheço nem desconheço
- Desconheço em parte
- Desconheço totalmente

Sabe se a Organização onde trabalha têm nomeado, formalmente, um Encarregado de Proteção de Dados interno ou externo? *

- Conheço totalmente
- Conheço em parte
- Não conheço nem desconheço
- Desconheço em parte
- Desconheço totalmente

Sabe em que situações/ocorrências dentro da sua Organização deve estar envolvido o EPD? *

- Conheço totalmente
- Conheço em parte
- Não conheço nem desconheço
- Desconheço em parte
- Desconheço totalmente

No seu ponto de vista e do que tem conhecimento o EPD atua em conformidade com o RGPD? *

- Conheço totalmente
- Conheço em parte
- Não conheço nem desconheço
- Desconheço em parte
- Desconheço totalmente

Na sua opinião quais as áreas que considera necessitarem de maior intervenção? *

- ☐ Adequação das políticas internas às disposições legais
- ☐ Formação aos colaboradores sobre o RGPD e os seus impactos
- ☐ Segurança física de Hardware e Software
- ☐ Salvaguarda de dados contra ameaças e ataques externos
- ☐ Definição de permissões e controlo de acessos aos dados
- ☐ Avaliação dos contratos com terceiros (clientes, fornecedores, etc.)

## Registo e Tratamento de dados

A Organização adaptou as políticas internas de acordo com as políticas estabelecidas pelo RGPD? *

- As políticas da empresa não estão formalizadas de acordo com o RGPD
- As políticas da empresa estão pontualmente de acordo com o RGPD
- Existe um conjunto de políticas formalizado e diversificado de acordo com práticas nacionais e internacionais
- Existe um conjunto de políticas implementadas e formalizadas de acordo com o RGPD

Tendo em conta os processos de proteção de dados existentes considera necessário serem feitas correções? *

- Será necessário criar os processos de proteção de dados
- São necessárias apenas algumas correções nos processos existentes
- São necessárias muitas correções nos processos existentes
- Não são necessárias correções

Considera que a sua Organização está preparada para gerir o acesso aos dados pessoais dos consumidores de acordo com o RGPD? *

- Está completamente preparada tanto para o acesso físico como para o acesso digital
- Está substancialmente mais preparada para a gestão do acesso físico do que do digital
- Está substancialmente mais preparada para a gestão do acesso digital do que do físico
- Não está preparada

Numa situação de incumprimento do RGPD tem conhecimento das penalidades aplicáveis? *

- Tenho conhecimento das penalidades e dos montantes máximos e mínimos previstos
- Tenho conhecimento das penalidades e apenas dos montantes máximos previstos
- Tenho conhecimento das penalidades, mas desconheço os montantes previstos
- Não sabia que existiam penalidades

Caso houvesse uma inspeção à implementação e aplicabilidade do RGPD na empresa onde trabalha considera que esta sofreria uma penalização financeira? *

- Sim
- Não Sei
- Não

## Consentimento do Consumidor

Responda numa escala de 1 a 7, em que: 1- Discordo totalmente; 2-Discordo parcialmente; 3-Discordo; 4- Não concordo nem discordo; 5- Concordo parcialmente; 6- Concordo; 7-Conconrdo totalmente

Estão definidos dentro da Organização procedimentos para a obtenção de consentimento junto do consumidor? *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|---|---|---|---|---|---|---|---|
| Discordo Totalmente | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Concordo Totalmente |

Os responsáveis pelo tratamento aplicam medidas técnicas para assegurar que, em regra, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento? *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|---|---|---|---|---|---|---|---|
| Discordo Totalmente | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Concordo Totalmente |

As medidas aplicam-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento e ao seu prazo de conservação? *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|---|---|---|---|---|---|---|---|
| Discordo Totalmente | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Concordo Totalmente |

Os procedimentos adotados asseguram que, em regra, os dados pessoais não sejam disponibilizados a um número indeterminado de pessoas singulares? *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|---|---|---|---|---|---|---|---|
| Discordo Totalmente | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Concordo Totalmente |

Nas atividades de recolha e registo de dados pessoais é fornecido a identidade e os contactos do responsável pelo tratamento e se for caso disso, do seu representante? *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|---|---|---|---|---|---|---|---|
| Discordo Totalmente | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Concordo Totalmente |

Quando os dados pessoais não são recolhidos junto do consumidor, o responsável pelo tratamento informa quais as finalidades do tratamento a que os dados se destinam? *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|---|---|---|---|---|---|---|---|
| Discordo Totalmente | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Concordo Totalmente |

Existem procedimentos de validação relativamente à obtenção dos consentimentos dos dados dos consumidores? *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|---|---|---|---|---|---|---|---|
| Discordo Totalmente | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Concordo Totalmente |