MANUAL PRÁTICO DO RGPD

PARA O CANAL HORECA

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

www.ahresp.com

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

MANUAL PRÁTICO DO RGPD

PARA O CANAL HORECA

Este Manual configura os principais procedimentos a ter em consideração, associados à adoção do Regulamento Geral de Proteção de Dados (RGPD), no âmbito do setor do Turismo e em particular no universo de Associados da **AHRESP**.

MANUAL PRÁTICO DO RGPD

PARA O CANAL HORECA

Síntese

O Manual que se apresenta contextualiza o âmbito de aplicação do Regulamento Geral de Proteção de Dados (RGPD), o qual, da responsabilidade da Comissão Europeia (CE), passou a figurar como instrumento de adoção obrigatória nos diversos Estados Membros, a partir de 25 de maio de 2018.

Por outro lado, apresenta igualmente as principais preocupações a ter em consideração, no que à utilização de dados pessoais se refere e às concomitantes obrigações atinentes à proteção e preservação dos mesmos, em salvaguarda dos direitos dos cidadãos no espaço europeu, seus únicos titulares.

Considerando o interesse dos associados da AHRESP, o Manual inclui ainda um conjunto de casos práticos que traduzem o conjunto de preocupações normalmente associadas a diferentes tipologias de associados, de acordo com a natureza da sua atividade, e o âmbito específico do RGPD, com vista ao apoio a proporcionar aos mesmos.

A utilização dos dados pessoais é hoje algo indispensável a qualquer negócio, em qualquer setor de atividade.

Interagir com os clientes, de forma direta e personalizada, é uma inegável mais valia que as tecnologias digitais vieram potenciar.

Assim, a adoção do RGPD pode ser uma oportunidade, depois de vencidas as barreiras inerentes à sua compreensão e especificidades de aplicação.

CONTEÚDO

1. O RGPD – Fundamentos 5

1.1. A razão de ser do RGPD 5

1.2. O que são "dados pessoais" 7

1.2.1. Dados pessoais em empresas do canal HORECA 8

1.3. O que significa "tratamento de dados" 9

1.3.1. As necessidades de tratar dados em empresas do canal HORECA 9

1.4. O que é um "ficheiro" e uma "Base de Dados" 10

1.4.1. Manutenção de dados em empresas do canal HORECA 10

1.5. As implicações do RGPD nas empresas do canal HORECA 11

2. Implementação do RGPD – Princípios e recomendações 14

2.1. A transformação digital na vida das empresas 14

2.2. Especificidades na implementação do RGPD 14

2.2.1. Garantir a conformidade com o RGPD 14

2.2.2. Efetuar o registo das atividades de tratamento 16

2.2.3. Nomear um EPD (Encarregado pela Proteção de Dados) 17

2.2.4. Cumprir com o direito de Acesso, Retificação, Cancelamento e Oposição (ARCO) 17

2.2.5. Garantir a inibição sobre o tratamento de dados sensíveis 18

2.2.6. Assegurar o exercício do direito a ser esquecido 18

2.2.7. Garantir a portabilidade dos dados 19

2.2.8. Inibir a criação de perfis 19

2.2.9. Garantir a proteção desde a conceção e por defeito 19

2.2.10. Segurança no tratamento e notificação 20

2.3. Boas práticas na implementação do RGPD em empresas do canal HORECA 20

3. A adoção do RGPD nos associados da AHRESP – Casos práticos 23

3.1. Check-list 23

3.2. Casos práticos 24

3.2.1. Caso "Pastealria Silva" (Nível 1) 24

3.2.2. Caso "Discoteca Bom Som" (Nível 2) 26

3.2.3. Caso "Aldeamento Sol, Mar e Ar Puro" (Nível 3) 29

4. Recomendações finais e contactos 33

4.1. Recomendações finais 33

4.2. Informações complementares 34

4.3. Contactos 35

5. ANEXOS 37

Mod.1 – Declaração de consentimento para uso de dados pessoais 37
Mod.2 – Acordo de Proteção de Dados 39

O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

1. O RGPD – FUNDAMENTOS

A digitalização dos negócios é hoje um dos principais desafios para as Organizações em qualquer setor de atividade. Viver numa sociedade em que a premissa da digitalização se afirmou como uma realidade incontornável, implica a necessidade de acompanhar esses desenvolvimentos, adquirindo as necessárias competências e adotando os procedimentos ajustados.

Neste quadro de referência, a Inovação e as Tecnologias de Informação (TI) assumem um papel preponderante, enquanto dinamizadores da transformação e dos processos de mudança associados ao digital.

A obrigatoriedade de adoção do Regulamento Geral de Proteção de Dados (RGPD), indissociável da Transformação Digital, implica uma **alteração de rotinas, desde logo de natureza administrativa, as quais estão relacionadas com o tratamento de dados pessoais**. Mas o RGPD representa também uma oportunidade de inovação, transversal a todas as organizações. Para o canal HORECA este é um desafio significativo, face à diversidade dos serviços prestados e às necessidades de aprofundar a relação com clientes, designadamente por via do emprego de estratégias de marketing digital, as quais dependem da existência de informação dos mesmos, identificando as suas preferências e hábitos de consumo.

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revogou a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), tendo sido tornado obrigatório em todos os Estados Membros da UE a partir de 25 de maio de 2018, consagrou que essas ações passaram a ser realizadas no estrito cumprimento dos mecanismo legais existentes, *i.e.*, a Lei 67/98 de 26 de outubro (Lei da Proteção de Dados Pessoais) e o próprio Regulamento, assegurando a privacidade e segurança dos dados fornecidos.

Importa assim reter alguns princípios fundamentais os quais passam a fazer parte da nomenclatura e dos procedimentos de todas as empresas. No essencial, o RGPD consagra a **adoção de uma nova cultura de mudança e uma oportunidade para a inovação por via do digital**, sendo para o efeito necessário que as organizações preparem e estabeleçam um plano consciente, adequado e sensato com vista à sua implementação.

Vejamos os fundamentos principais do RGPD, desde logo relativamente à clarificação de um conjunto de conceitos, cujas definições constam do Artº 4º, que reedita as que já tinham sido estabelecidas pela Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 e transportas para a ordem jurídica nacional através da Lei 67/98 de 26 de outubro.

1.1. A RAZÃO DE SER DO RGPD

A livre circulação de bens, serviços, pessoas e capitais no espaço da União Europeia (UE), visa, entre outros objetivos de salvaguarda de direitos e liberdades, a consagração de um mercado interno, numa perspetiva de prosperidade e liberdade proporcionada a 500 milhões de cidadãos europeus. Insere-se neste mesmo contexto a criação de um mercado único digital, no qual pessoas e empresas possam realizar as suas operações de oferta, aquisição e consumo de produtos e/ou serviços em ambiente digital.

A construção de um mercado único digital encerra diversos desafios, em que um dos mais sintomáticos se prende com a licitude da informação que circula / partilha, em particular quando esta viola o direito à privacidade de qualquer pessoa.

Sendo um dos direitos fundamentais de qualquer cidadão, a privacidade individual insere-se no âmbito da garantia da integridade, identidade e dignidade de cada pessoa, sendo por isso protegida por lei.

A decisão da Comissão Europeia (CE), tomada em 2017, de que os cidadãos europeus passariam a ter acesso livre a conteúdos digitais subscritos em qualquer dos estados membros, estabeleceu de modo inequívoco a existência de uma dimensão digital da identidade de cada indivíduo. No espaço da UE, qualquer cidadão de um estado membro passou assim a ter direito a desfrutar da sua experiência digital, regular, independentemente do país onde se encontrasse. Ao ter dado esse novo passo em direção a um processo de transformação digital, a CE reconheceu que essa alteração, não sendo confinada a uma distância geográfica, compreendia um direito inerente a cada cidadão, a par do de livre circulação. Neste sentido, o Regulamento é aplicável aos responsáveis pela realização de tratamentos de dados pessoais que se encontrem estabelecidos na UE, ou seja, por qualquer empresa que determine as finalidades e os meios pelos quais o mesmo se realize, seja este efetuado pelos seus próprios meios ou em conjunto com uma ou mais entidades terceiras (subcontratantes), estando estas igualmente sujeitas ao seu cumprimento quando estejam estabelecidas na UE, ou quando o tratamento de dados pessoais em causa estiver relacionado com ofertas de bens ou serviços a cidadãos da UE, ou ao controlo do comportamento desses cidadãos na UE.

A "identidade" digital de cada cidadão é uma nova realidade que se insere na esfera da individualidade de cada pessoa e, por essa razão, deve ser compreendida como uma "extensão" da defesa do direito à sua integridade, em que a privacidade é um pilar fundamental.

Assim, o RGPD, no seu enquadramento, refere que:

> *(1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.o, n.o 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.o, n.o 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.*
>
> *(2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.*

Sendo esse o escopo fundamental do RGP, fica implícita a obrigatoriedade das empresas em estabelecerem métodos de suporte às possíveis atividades de recolha, armazenamento e processamento de dados pessoais que desenvolvam, independentemente de serem realizados

pelas próprias empresas ou através de entidades contratadas para o efeito, como antes referido, bem como a estabelecerem os mecanismos de controlo do seu próprio funcionamento interno.

De realçar que a obrigatoriedade das empresas implica, designadamente, que o sistema anteriormente existente de notificações e autorizações prévias, deixa de existir. Sendo esse sistema caracterizado pelo pedido de autorização prévia apresentado junto da Comissão Nacional de Proteção de Dados (CNPD), passarão a ser as próprias empresas que tratam dados pessoais a ajuizar se determinado tratamento é lícito ou não uma vez que este regulador passa passar a ser, essencialmente, uma autoridade de fiscalização.

Para a realização desse exercício têm as empresas de analisar qual o impacto decorrente do tratamento de dados pessoais que realizem, ou pretendam vir a realizar, para a privacidade dos cidadãos envolvidos, bem como decidir sobre que medidas devem aplicar, considerando as medidas de segurança a serem implementadas, salvaguardando a integridade, confidencialidade e disponibilidade dos dados tratados.

1.2. O QUE SÃO "DADOS PESSOAIS"

O Regulamento estabelece como dados pessoais: qualquer *informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*.

Assim, **entendem-se como dados pessoais qualquer tipo de registo informativo, texto, som ou imagem (fixa ou animada), em qualquer suporte, como seja em papel ou digital, que permita saber e/ou identificar quem é uma determinada pessoa, sendo este o único titular dos mesmos, ou seja, "*é o legítimo dono dos dados que ao próprio dizem respeito*"**. Nesse sentido, um formulário com informação sobre cada pessoa, bem como fotografias com um campo com a identificação de quem se encontra representado, entre outras formas, são mecanismos de recolha / registo de dados pessoais.

Importa reforçar que existem **identificadores diretos**, como sejam o nome, um número (Ex: CC ou NIF), um endereço de email, entre outros, bem como **identificadores indiretos**, os quais resultam de um conjunto de elementos (dados) sobre uma pessoa, os quais, por si só, não permitem identificar ninguém, mas que em conjunto permitem saber de quem se trata. As obrigações sobre proteção de dados decorrentes do RGPD incidem sobre ambas as situações.

O RGPD é particularmente incisivo sobre determinado tipo de **dados, designados como sensíveis**, os quais devem estar sujeitos a condições de tratamento específicas, visando uma proteção acrescida sobre os mesmos, prevenindo o risco de quebra de privacidade. Dados sensíveis são todos aqueles que se referem:

- À origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas;
- À filiação sindical;
- A dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano;
- A dados relacionados com a saúde;
- A dados relativos à vida sexual ou orientação sexual da pessoa.

1.2.1. Dados pessoais em empresas do canal HORECA

A recolha de dados por parte da generalidade das empresas no canal HORECA é hoje uma realidade transversal a todas as áreas de negócio, seja esta diretamente realizada pelos próprios hotéis, hostels ou restaurante, entre outros, ou por entidades subcontratadas para esse efeito. A conveniência em assegurar informação sobre os clientes como suporte ao processo de contacto e de manutenção de uma relação com os mesmos é tida como um fator fundamental, sendo este tanto mais relevante quanto maior for a empresa ou mais extensa for a natureza dos serviços prestados.

Sendo assim prática corrente a recolha, tratamento e manutenção de arquivos com dados sobre clientes, é importante distinguir entre dados referentes a clientes empresariais e dados sobre clientes individuais:

- Dados associados a clientes empresariais – o princípio a ser aplicado é o de que não existem obrigatoriedades específicas quando a natureza dos dados a serem recolhidos e tratados é apenas de âmbito empresarial (pessoa coletiva). No entanto, sempre que forem recolhidos dados sobre pessoas de contacto nesses clientes, aplicam-se os princípios do RGPD, considerando a integridade, confidencialidade e acessibilidade desses mesmos dados pessoais. Neste âmbito, sendo compreensível a recolha de dados de contacto (Ex: Nome, nº de telefone de serviço, de email profissional e eventualmente do cargo), já pode ser questionável a natureza/extensão e tratamento de outros dados (Ex: Dados sensíveis), bem como o tratamento de todos os dados recolhidos. Assim, caso um hotel, hostel ou restaurante, entre outros, possua apenas dados sobre clientes empresariais, não terá de adotar nenhuma atitude específica, o mesmo já não se passando quando possua registos sobre pessoas individuais associadas a esses clientes;
- Dados sobre clientes individuais – no caso do tratamento de dados ser referente a pessoas individuais, devem os hotéis, hostels ou restaurantes, entre outros, garantir o cumprimento do RGPD, seja este tratamento efetuado diretamente por essas empresas ou por via de entidades por si subcontratadas.

Em qualquer dos casos, a existirem dados pessoais associados a clientes, os titulares dos mesmos deverão ter prévio conhecimento da sua existência, sendo fundamental que autorizem a sua recolha, bem como a sua utilização, em particular quando a mesma for para além do mero contacto decorrente da relação comercial existente e sempre que incluir ações de divulgação / promoção dos serviços prestados pela empresa do canal HORECA.

Para além dos dados pessoais referentes a clientes qualquer hotel, restaurante ou similar, tem de tratar dados sobre os seus colaboradores/funcionários (1.4), cumprindo-se para os mesmos idênticas obrigações. Ou seja, não sendo questionável a necessidade de recolha dos mesmos para efeitos das obrigações da empresa, quer perante os titulares dos mesmos, quer para com os serviços do Estado, deverá, no entanto, ter particular atenção com os aspetos referentes à integridade, confidencialidade e acessibilidade dos mesmos, em particular quando estes incluírem dados sensíveis. Nesse sentido, deverão as empresas do canal HORECA informar os seus colaboradores/funcionários sobre as finalidades da recolha de dados, solicitando a autorização prévia sempre que, quer pela natureza dos dados ou pelo tratamento dos mesmos, se justifique.

1.3. O QUE SIGNIFICA "TRATAMENTO DE DADOS"

O Regulamento também refere que se deve entender como tratamento de dados, *uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição* dos mesmos.

De acordo com a definição, **existe tratamento de dados quando se realizam intervenções sobre registos informativos acerca de pessoas individuais, incluindo as que decorrem de atos humanos, sem recurso a meios informáticos**. Nesse sentido, a manutenção de um dossiê em papel, onde são arquivadas por ordem sequencial de número atribuído, ou por outra forma, fichas com informação de clientes e/ou pessoas individuais, é considerado tratamento de dados.

1.3.1. As necessidades de tratar dados em empresas do canal HORECA

A atividade de hotéis, restaurantes e similares, inscrevendo-se no âmbito do setor do Turismo, caracteriza-se pela prestação de serviços em que a fruição de sensações de bem-estar se configuram como o objeto principal das diferentes propostas de valor. Dirigindo a sua oferta a indivíduos nas suas mais diversas "combinações" (Ex: Solteiros, Jovens, Casados, Seniores, etc), as empresas do setor do Turismo têm hoje, como um dos seus principais ativos, a recolha e tratamento de dados sobre os seus grupos-alvo, criando uma maior proximidade com os mesmos, designadamente para efeitos da construção de propostas de valor mais ajustadas aos interesses desses. Assim, essas empresas devem, de um modo geral, ponderar seriamente sobre a necessidade de implementarem as adequadas medidas, atendendo à crescente necessidade de recolherem e tratarem dados pessoais.

Associadamente, de modo a comprovar o cumprimento com as normas do Regulamento, deverão essas empresas, através dos responsáveis pelo tratamento desses dados (2.2.3), ou dos seus representantes, efetuar e manter registos escritos desses atos (em suporte papel ou eletronicamente), disponibilizando-os à CNPD sempre que for para o efeito solicitado (2.2.2). No entanto, poderão estar dispensadas desta formalidade quando, cumulativamente: i) tiverem menos de 250 trabalhadores: ii) apenas efetuarem tratamentos de dados que não sejam suscetíveis de implicar um risco para os direitos e liberdades dos seus titulares; iii) tratarem dados de modo ocasional (sem regularidade); e iv) não tratarem quaisquer dados considerados sensíveis ou relativos a condenações penais e infrações. São, assim, diversas as empresas do setor do turismo que estão sujeitas a esta obrigação (manutenção de registos adequados). Malgrado, ainda que uma determinada empresa não reúna qualquer dos requisitos acima (Ex: Um pequeno restaurante), é recomendável que mantenha um registo, ainda que simplificado, das atividades de tratamento de dados que efetue, demonstrando o cumprimento das suas demais obrigações e facilitando o seu contacto com a CNPD, em caso de fiscalização.

Atendendo à responsabilidade que o Regulamento acarreta sobre todas as empresas que efetuem a recolha e tratamento de dados pessoais, é prudente e recomendável proceder à nomeação de alguém responsável pelos mesmos (Encarregado da Proteção de Dados), mesmo que tal não seja obrigatório no caso concreto (2.2.3). O Encarregado da Proteção de

Dados que seja nomeado voluntariamente será, todavia, sujeito ao mesmo estatuto de um Encarregado que tivesse sido nomeado por força do Regulamento.

1.4. O QUE É UM "FICHEIRO" E UMA "BASE DE DADOS"

Com vista a uma completa clarificação de conceitos o Regulamento estabelece ainda diversas definições, designadamente o que se entende como ficheiro. Assim, ficheiro é um ***qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico***. Assim, sublinha-se que **os ficheiros podem ser de natureza digital, mas também em papel, sendo válidos os artigos arquivadores**. Estes, organizavam-se em pequenas fichas com informação preenchida, ou impressa, normalmente por ordem alfabética, ou crescente (numérica).

Hoje, é mais normal pensar em Bases de Dados quando nos referimos a organização de informação, sendo estas realidades digitais, quer porque a informação original já tem essa natureza, quer porque decorre da *digitalização* de informação em papel. **As Bases de Dados são modelos de organização de informação em ambiente informático, sendo acessíveis sobre diversas formas**.

O Decreto Lei n.º 122/2000, de 04 de julho, que transpôs para o ordenamento jurídico nacional a Diretiva n.º 96/9/CE, do Parlamento Europeu e do Conselho, de 11 de Março, relativa à proteção jurídica das bases de dados, refere que se entende por base de dados a *coletânea de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e suscetíveis de acesso individual por meios eletrónicos ou outros*.

Resta acrescentar que a generalidade das organizações tem informação organizada sobre os seus colaboradores, as quais possibilitam o acesso direto a determinados dados sobre os mesmos. A necessidade de existirem Bases de Dados sobre funcionários/colaboradores é inequívoca e devidamente justificada pela obrigatoriedade das organizações cumprirem com as suas obrigações perante os mesmos, como seja para pagamento de salários e subsídios, mas também perante a administração tributária e a segurança social. Assim, não estando em causa o registo de dados fundamentais para as obrigações acima descritas, entre outras, já quanto a outros dados cumprem-se as demais responsabilidades previstas no RGPD.

1.4.1. Manutenção de dados em empresas do canal HORECA

É importante ter presente que a existência, por muito pouco provável que possa parecer, de arquivos de dados organizados em suporte papel, designadamente com a possibilidade de serem realizadas consultas por ordem alfabética, são tão considerados como são as Bases de Dados informáticas. Assim, um clássico arquivo com fichas/cartões de cliente em suporte de papel, nas quais se incluam dados pessoais, como os referidos em 1.2.1, está sujeito ao cumprimento do RGPD.

Da mesma forma, quando a informação dos dados pessoais sobre clientes se encontre registada através de uma folha de Excel, uma Tabela, ou mesmo uma Lista, em Word, a mesma encontra-se sujeita a idênticas obrigações. Apenas não seria obrigatório qualquer procedimento relacionado com o RGPD se os dados pessoais existentes não fossem passíveis de ser consultados, designadamente por inexistência dum qualquer sistema de indexação ou de estabelecimento de relacionamento entre os mesmos, tornando impossível a pretensão de querer saber quem era quem, em cada momento de consulta/pesquisa.

Neste sentido, qualquer estabelecimento de restauração, hotel, ou outro similar, que tenha uma forma organizada de acesso a dados pessoais sobre os seus clientes, deverá cumprir com as determinações do RGPD, sendo válidos esses mesmos princípios no que se refere a dados sobre colaboradores/funcionários desses estabelecimentos.

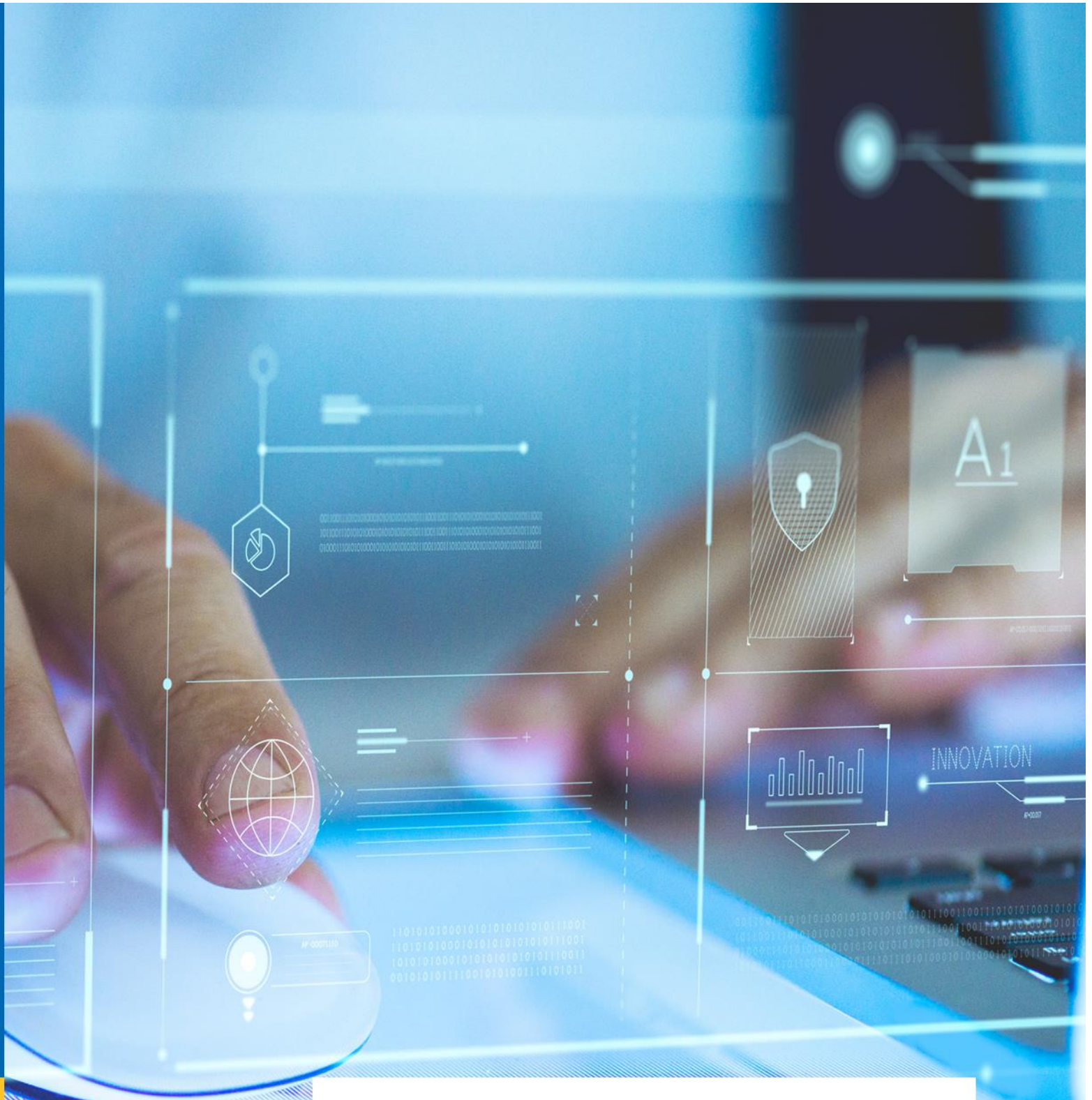
1.5. AS IMPLICAÇÕES DO RGPD NAS EMPRESAS DO CANAL HORECA

A adoção do RGPD, obrigatória desde 25 de maio de 2018, traz implicações para hotéis, hostels, restaurantes ou quaisquer outras entidades que prestem serviços no âmbito do canal HORECA:

- **Todas as empresas do canal HORECA (grandes, médias ou pequenas empresas) que façam o tratamento de dados pessoais estão sujeitas a este regime**, independentemente da sua natureza jurídica, designadamente de serem pessoas singulares ou coletivas, ou do âmbito das suas atividades. Salvaguardando situações muito pontuais, **o princípio é o de que ninguém está excluído da sua aplicação**, no entanto, aqueles que dependem dum maior grau de dados pessoais serão, necessariamente, mais afetados. Nesse sentido, casos como as cadeias de hotéis e/ou de estabelecimentos de restauração, estarão mais sujeitas a essas determinações, designadamente por força do número de dados recolhidos e pela necessidade de tratamento regular dos mesmos;
- **As empresas do canal HORECA devem realizar a avaliação das práticas existentes e associadas ao tratamento de dados pessoais existente**, devendo desenhar e implementar os adequados processos para a necessária implementação do RGPD, considerando as metodologias, suportes documentais e afetação de recursos, designadamente de pessoas;
- As empresas do canal HORECA deverão partilhar a informação sobre as suas práticas – **Política de Privacidade e de Proteção de Dados** – com os titulares de dados, as quais deverão ser elaboradas no estrito cumprimento do RGPD, considerando a especificidade de cada realidade empresarial, conforme se refere em 2.2;
- **As empresas do canal HORECA deverão providenciar e garantir a necessária adequação das tecnologias utilizadas**, seja por via direta, seja através da prestação de serviços dos seus fornecedores, relativamente às dimensões técnicas e organizativas, com particular relevância em termos da segurança dos dados e da mitigação de riscos em aspetos diversos, como sejam os referentes à pseudonimização[1] dos dados pessoais, à implementação de mecanismos de confidencialidade, à integridade e disponibilidade desses dados, bem como à resiliência dos próprios sistemas informáticos;
- Com o RGPD **as empresas do canal HORECA passam a ser diretamente responsáveis** pela sua correta aplicação, designadamente perante a autoridade de controlo nacional – Comissão Nacional de Proteção de Dados (CNPD) – tendo, nalguns casos, de nomear um responsável pela sua correta aplicação e manutenção dos diversos procedimentos associados (EPD – Encarregado da Proteção de Dados);
- Com o RGPD **qualquer empresa passa a estar sujeita à aplicação de coimas diretas, as quais podem atingir o valor máximo de 20 milhões de euros ou, até 4% do volume de negócios anual**, considerando para efeitos de cálculo o apuramento a nível mundial, correspondente ao exercício financeiro anterior, considerando o montante mais elevado;

[1] Tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

- Por último, importa salientar que a adoção do RGPD traz uma mudança de paradigma e na cultura das organizações, de um modo geral, relativamente à forma como se lida com dados pessoais e que se compreendem os seus impactos, seja para o negócio, seja para os titulares dos mesmos, o que obrigará a um esforço de adaptação que perdurará para sempre na vida das empresas.



IMPLEMENTAÇÃO DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

AHRESP
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

2. IMPLEMENTAÇÃO DO RGPD – PRINCÍPIOS E RECOMENDAÇÕES

Atentemos agora, de modo mais detalhado, nas principais preocupações que devem estar subjacentes a qualquer empresa, na adoção do RGPD, considerando um conjunto de princípios e recomendações transversais.

2.1. A TRANSFORMAÇÃO DIGITAL NA VIDA DAS EMPRESAS

Vivemos hoje um processo de Transformação Digital (DX, na designação inglesa). Este processo prende-se com o facto de que a vida das empresas está cada vez mais interconectada com as tecnologias digitais, seja por via da dependência das plataformas em linha (*online*), seja através da aplicação de aplicações digitais como suporte a processos diversos, desde logo de relacionamento e criação de proximidades com clientes. Nenhuma empresa pode passar ao lado de que os desenvolvimentos mais recentes, em termos de armazenamento e capacidade de processamento de grandes volumes de informação, do desenvolvimento de *cloud services*, da generalização das soluções de *mobile computing*, das Redes Sociais e do concomitante e exponencial desenvolvimento do *Big Data*, têm criado a necessidade de repensar processos e de desenvolver novas abordagens e posicionamentos estratégico.

Esta realidade, sendo também particularmente sentida nas atividades económicas inseridas no setor do Turismo, é especialmente relevante no âmbito da Hotelaria / Hospedagem e da Restauração, onde a criação de valor aparece cada vez mais associada ao estabelecimento de relações de confiança com os clientes, os quais dispõem hoje de uma multiplicidade de meios nos quais podem aferir da qualidade dos serviços prestados, intervindo de modo direto na perceção que os outros possam ter sobre os mesmos. Assim, a criação de uma estratégia para o digital, na qual a exploração desse potencial tecnológico deve ser equacionada de modo sistemático e construtivo, tem hoje diversas implicações para as unidades de negócio que constituem o setor do Turismo, muitas vezes com implicações ao nível do próprio modelo de negócios. Neste sentido, a consolidação de uma estratégia para o digital, assume hoje particular acuidade.

Nas empresas no setor da Hotelaria e da Restauração existem bases de dados, ou arquivos, com informação sobre clientes, sendo essa uma informação relevante para qualquer negócio. A capacidade de gerir os interesses dos clientes de hotéis, hostels, restaurantes ou de outras unidades de negócio, acrescentando valor através da valorização de produtos/serviços e do aumento da lealdade dos mesmos para com essas ofertas, é o objetivo fundamental de qualquer processo de "gestão da carteira de clientes". Nesse sentido, a capacidade de tratar digitalmente esta informação é hoje um pressuposto fundamental dada a necessidade permanente de conhecer cada cliente e de estabelecer as melhores estratégias de comunicação com os mesmos.

2.2. ESPECIFICIDADES NA IMPLEMENTAÇÃO DO RGPD

Salvaguardando o facto de que o RGPD prevê a derrogação de alguns aspetos para micros e PME's, tendo a possibilidade dos Estados Membros elaborarem procedimentos específicos em setores e situações justificadas, façamos uma análise geral dos principais aspetos a ter em consideração na adoção do RGPD, considerando as implicações em termos de pessoas, de processos e de meios tecnológicos subjacentes.

2.2.1. Garantir a conformidade com o RGPD

A necessidade que as empresas passem a estar em conformidade com o RGPD incide na demonstração prática, e visível, da **existência de uma política e de processos**

implementados para o efeito (medidas técnicas e organizativas), sendo o primeiro e verdadeiramente essencial, o de consentimento prévio, através do qual se pretende dar conhecimento ao titular de dados sobre as atividades, extensão e implicações do respetivo tratamento, solicitando a sua autorização.

Muitas das práticas existentes enfermam de incorreções e até mesmo de ilegalidades, uma vez que não agem de acordo com o definido, decorrendo esses princípios, designadamente, da Diretiva 93/13/CEE do Conselho que consubstancia o tipo de prática/cláusula que pode ser considerada como abusiva na relação contratual com consumidores. O Regulamento estabelece que "*sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados*… [devendo*] existir as devidas garantias de que… está plenamente ciente do consentimento dado e do seu alcance*". Para o efeito deverá ser fornecida uma declaração de consentimento (Anexos – Mod.1), a qual deverá ser "*inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado*".

Deve igualmente ter-se em consideração que se presume que "*o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução*".

Significa assim **que o tratamento de dados não pode ser realizado sem o consentimento explícito do titular de dados**, devendo o respetivo titular autorizar os atos subjacentes ao tratamento, através de documento específico, o qual deve ser redigido de forma clara e abrangente. Saliente-se que o consentimento para determinados atos de tratamento de dados, podendo ser necessário para determinados fins, pode violentar os princípios de privacidade e obtenção de consentimento prévio, se os mesmos condicionarem, indevidamente/ilicitamente, a prestação de serviços.

Os dados devem ser exatos e apenas conservados durante o período necessário, sendo obrigatoriamente eliminados após esse período. Devem existir meios tecnológicos que garantam a devida proteção, designadamente prevenindo o acesso e utilização indevida, a sua perda, bem como a danificação e/ou destruição parcial ou total. Com exceção de algumas situações, o princípio geral é o de que o titular dos dados tem de ter conhecimento prévio e explicitamente autorizar a recolha e tratamento dos mesmos, conforme já referido. Uma das implicações desta obrigação, entre outras, faz com que as organizações passem a informar que os seus *sites* recolhem informação sobre a navegação que os utilizadores fazem nos mesmos, os designados *cookies*[2], tendo de solicitar o consentimento explícito para o efeito (*opt-in*), ao invés da prática antes generalizada de apenas facultarem a possibilidade dos utilizadores se excluírem dessa circunstância (*opt-out*).

[2] *Cookies* são etiquetas de software armazenadas em cada computador através do navegador (browser), que retêm informação relacionada com as preferências de navegação em cada *site*.

As empresas no âmbito do canal HORECA, têm assim de definir as especificidades que cada uma considere ser ajustada à recolha e tratamento que realize sobre os dados pessoais dos seus clientes, bem como da utilização que pretendem fazer desses mesmos dados, dando-o a conhecer a cada cliente de forma explícita e inequívoca, possibilitando que os mesmos autorizem (previamente) a respetiva utilização, caso a caso. Para o efeito deverá garantir a existência da informação adequada, solicitando a sua concordância/consentimento, registando-a através de documento próprio (Anexos – Mod.1).

2.2.2. Efetuar o registo das atividades de tratamento

O RGPD (Artº 30º) obriga ao registo das atividades de tratamento, o qual deve ser realizado, tanto pelos responsáveis do mesmo, e sendo caso disso pelo seu representante, bem como pelos subcontratantes, e sendo caso disso pelo(s) representante(s) deste(s), competindo-lhe(s) a realização e conservação de um registo (documental) de todas as atividades de tratamento sob a sua responsabilidade. Estes devem, sempre que para o efeito forem solicitados, disponibilizar esses documentos à CNPD.

Devem ser documentadas de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação de manter um registo como as relativas a outros procedimentos internos, de modo a que as organizações estejam aptas a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD (*accountability*).

As obrigatoriedades de realizar e conservar registos das atividades relacionadas com o tratamento de dados sob responsabilidade, *não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9º, nº 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10º*, conforme enunciado no Artº 30º, nº 5.

Conforme antes referido (1.3.1), e apesar de a obrigatoriedade de registo das atividades de tratamento não ser aplicável a muitas das empresas no canal HORECA, é recomendável que as mesmas mantenham registo, ainda que simplificado, das atividades de tratamento de dados que efetuem, demonstrando que cumprem com as suas obrigações, respeitando o âmbito do mesmo e assegurando a integridade, identidade e dignidade de cada titular de dados (cliente), cumprindo com as suas demais obrigações e facilitando, desse modo, o contacto com a CNPD, em caso de fiscalização.

As atividades de tratamento devem ser registadas de forma clara e elucidativa, aplicando-se, quando for caso disso, quer a hotéis, hostels, restaurantes ou similares, bem como aos subcontratantes (sempre que existam). A CNPD disponibiliza instrumentos de suporte ao cumprimento das obrigações de registo (tabelas de registo), quer por parte do responsável pelo tratamento, quer pelos subcontratantes, podendo os mesmos serem adotados pelos operadores de Turismo[3].

[3] https://www.cnpd.pt/bin/rgpd/rgpd.htm

2.2.3. Nomear um EPD (Encarregado pela Proteção de Dados)

A nomeação de um EPD (Encarregado pela Proteção de Dados), ou DPO (*Data Proteccion Officer)* na terminologia inglesa, é referida no RGPD (Artº 37º), como sendo um ato a ser realizado pelo **responsável pelo tratamento,** ou seja, *a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais*, e o **subcontratante,** ou seja, *a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes*, designam um encarregado da proteção de dados, o qual passará a estar envolvido em todas as questões relacionadas com a proteção de dados pessoais. Esta função deve ser atribuída **sempre que o processamento for levado a cabo por uma entidade pública**, se verifique a necessidade de **tratar dados pessoais em grande escala e de forma constante** (Ex: Bancos ou empresas de telecomunicações), ou exista **processamento de dados sensíveis em larga escala**.

As principais funções do encarregado de proteção de dados envolvem: 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, que inclui, por exemplo, formar a equipa e realizar auditorias relacionadas com esta área; iv) e cooperar e atuar como ponto de contacto com as autoridades de proteção de dados.

Conforme fica claro, a obrigatoriedade da nomeação de um EPD não se verifica na grande maioria dos casos do tecido empresarial nacional, constituído por PME's e micro-empresas, atendendo a 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, conforme já referido (1.4.1), é de todo recomendável que empresas no âmbito do canal HORECA que vejam excluída essa obrigatoriedade, mas cuja atividade implique o tratamento de dados pessoais, nomeiem alguém responsável pelo cumprimento das demais obrigações do RGPD, assegurando os necessários cuidados e a salvaguarda de direitos dos titulares de dados, bem como de eventual contacto com a CNPD.

2.2.4. Cumprir com o direito de Acesso, Retificação, Cancelamento e Oposição (ARCO)

As empresas devem informar os titulares dos dados e prever a existência de mecanismos que possibilitem que cada um possa aceder à informação existente sobre si, solicitar que a mesma seja retificada e/ou cancelada, se designadamente a considerar desapropriada para os fins visados, podendo ainda estabelecer oposição às práticas de gestão de dados da empresa, designadamente por via judicia e/ou através da CNPD.

Para esse efeito, as empresas no canal HORECA, deverão adotar procedimentos simples, mas explícitos e elucidativos, os quais deverão ser dados a conhecer aos titulares de dados (clientes), desde logo sobre os direitos ARCO que lhes assistem. Para o efeito poderão/deverão incluir essa informação na Declaração de Consentimento a ser assinada pelos próprios (Anexos – Mod.1).

2.2.5. *Garantir a inibição sobre o tratamento de dados sensíveis*

Existem categorias de dados considerados de natureza sensível, como sejam os relativos à origem racial ou étnica de uma pessoa, às suas opiniões políticas e convicções religiosas ou filosóficas, à filiação sindical, bem como dados sobre o padrão genético e biométricos que permitam identificar uma pessoa de forma inequívoca e ainda dados relativos à vida sexual ou orientação sexual de uma pessoa. O tratamento destes dados fica proibido sempre que os mesmos sejam reveladores da identidade de uma pessoa, a não ser que seja previamente autorizado pelo próprio ou em determinadas condições e para fins específicos, como sejam no âmbito de consultas por serviços médicos.

Significa assim, que o responsável pelo tratamento de dados ou subcontratante, em qualquer empresa do canal HORECA, deverá prevenir qualquer possibilidade de que, utilizadores não autorizados, possam vir a identificar qualquer pessoa através do acesso a dados sensíveis (indicadores indiretos).

Atendendo à complexidade de algumas destas intervenções, desde logo pela possibilidade de desenvolvimento de soluções que incorporem o uso de Tecnologias de Informação (TI), pode ser necessária a subcontratação de serviços especializados, devendo serem salvaguardas as cláusulas que assegurem o cumprimento do RGPD por parte desses prestadores de serviços (Anexos – Mod.2).

2.2.6. *Assegurar o exercício do direito a ser esquecido*

O titular de dados pode solicitar que sejam apagados os seus dados, devendo para o efeito o responsável pelo tratamento dos mesmos, ou subcontratante, acionar os necessários mecanismos tecnológicos para o efeito. Tal procedimento implica: i) apagar os respetivos registos das bases de dados em que os mesmos existam; ii) comunicar a todas as partes envolvidas (terceiros) que o devem igualmente fazer, designadamente aos que tenham tido acesso aos mesmos em consequência de ações anteriores, desde logo em termos de comunicação pública.

Excetuam-se desta obrigação, as situações por razões de exercício da liberdade de expressão e de informação, cumprimento de obrigações legais, exercício de funções de interesse público ou por autoridade pública, para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos em determinadas situações, ou ainda para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Para esse efeito, as empresas no canal HORECA, deverão adotar procedimentos simples, mas explícitos e elucidativos, os quais deverão ser dados a conhecer aos titulares de dados (clientes), desde logo sobre o designado “direito ao esquecimento” que lhes assistem. Para o efeito poderão/deverão incluir essa informação na Declaração de Consentimento a ser assinada pelos próprios (Anexos – Mod.1).

Por outro lado, atendendo à complexidade de algumas das intervenções que são necessárias para garantir o cumprimento desse direito, desde logo pela possibilidade de desenvolvimento de soluções que incorporem o uso de TI, pode ser necessária a subcontratação de serviços especializados, devendo serem salvaguardas as cláusulas que assegurem o cumprimento do RGPD por parte desses prestadores de serviços (Anexos – Mod.2).

2.2.7. *Garantir a portabilidade dos dados*

O titular de dados pode solicitar que lhe sejam entregues os mesmos num formato estruturado, de uso corrente e de leitura automática, desde logo em suporte eletrónico, bem como solicitar a sua portabilidade, podendo requerer que esta seja realizada por meios igualmente eletrónicos, desde que disponíveis para o efeito.

Para esse efeito, as empresas no canal HORECA, deverão adotar procedimentos simples, mas explícitos e elucidativos, os quais deverão ser dados a conhecer aos titulares de dados (clientes). Para o efeito poderão/deverão incluir essa informação na Declaração de Consentimento a ser assinada pelos próprios (Anexos – Mod.1).

Por outro lado, atendendo à complexidade de algumas das intervenções que são necessárias para garantir o cumprimento desse direito, desde logo pela possibilidade de desenvolvimento de soluções que incorporem o uso de TI, pode ser necessária a subcontratação a subcontratação de serviços especializados, devendo serem salvaguardas as cláusulas que assegurem o cumprimento do RGPD por parte desses prestadores de serviços (Anexos – Mod.2).

2.2.8. *Inibir a criação de perfis*

Salvaguardando algumas exceções, o titular de dados tem o direito de se opor a tratamentos automatizados a partir da criação de perfis decorrentes da sua relação com a empresa. Significa assim que as empresas não poderão realizar o processamento automatizado de informação pessoal, com o objetivo de avaliar e tipificar indivíduos com base nos seus dados pessoais, salvo autorização, expressa, dos próprios para esse efeito.

Para esse efeito, as empresas no canal HORECA, deverão adotar procedimentos simples, mas explícitos e elucidativos, os quais deverão ser dados a conhecer aos titulares de dados (clientes). Para o efeito poderão/deverão incluir essa informação na Declaração de Consentimento a ser assinada pelos próprios (Anexos – Mod.1).

Por outro lado, atendendo à complexidade de algumas das intervenções que são necessárias para garantir o cumprimento desta obrigatoriedade, desde logo pela possibilidade de desenvolvimento de soluções que incorporem o uso de TI, pode ser necessária a subcontratação de serviços especializados, devendo serem salvaguardas as cláusulas que assegurem o cumprimento do RGPD por parte desses prestadores de serviços (Anexos – Mod.2).

2.2.9. *Garantir a proteção desde a conceção e por defeito*

Devem ser aplicadas as medidas técnicas e organizativas adequadas, como sejam as de pseudonimização e de minimização, destinadas a garantir a eficácia dos princípios da proteção de dados, como sejam as relacionadas com o anonimato e a utilização de dados pessoais limitados ao que é estritamente necessário para as finalidades para as quais são tratados. Significa assim que as medidas técnicas e organizativas a aplicar devem assegurar que, por defeito, só sejam tratados os dados pessoais que sejam necessários para cada finalidade específica do tratamento, tanto em termos da quantidade de dados pessoais recolhidos, como relativamente à extensão do seu tratamento, ao seu prazo de conservação e ainda à sua acessibilidade. Estas medidas devem ainda salvaguardar que, por defeito, os dados pessoais não possam ser acedidos por um número indeterminado de pessoas.

Atendendo à complexidade subjacente para garantir o cumprimento desta responsabilidade, desde logo pela possibilidade de desenvolvimento de soluções que incorporem o uso de TI, pode ser necessária a subcontratação de serviços especializados, devendo serem salvaguardas as cláusulas que assegurem o cumprimento do RGPD por parte desses prestadores de serviços (Anexos – Mod.2).

2.2.10. Segurança no tratamento e notificação

Tendo como referências as técnicas mais avançadas, devem as organizações de aplicar as medidas técnicas e organizativas necessárias para garantirem um nível de segurança adequado ao risco, incluindo a possibilidade de pseudonimização e de cifragem dos dados, a confidencialidade, integridade, resistência e o adequado funcionamento dos sistemas, bem como o restabelecimento e acessibilidade aos dados em tempo adequado, em função de incidentes físicos ou técnicos. Devem assim adotar procedimentos de monitorização regular que garantam a segurança no tratamento de dados pessoais, prevenindo a ocorrência de incidentes de segurança ao nível das redes e dos sistemas de informação, bem como de situações de violação de dados (de forma acidental ou intencional), podendo estas ter graves consequências ao nível da destruição, da perda, da alteração, da divulgação ou do acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Sempre que se verifiquem situações de violação dos dados, deverá o responsável pelo tratamento notificar a autoridade de controlo competente (máx. 72h), bem como o titular dos mesmos, nas situações em que as violações sejam suscetíveis de implicar um elevado risco para os direitos e liberdades dos titulares.

Atendendo à complexidade subjacente para garantir o cumprimento desta responsabilidade, desde logo pela possibilidade de desenvolvimento de soluções que incorporem o uso de TI, pode ser necessária a subcontratação de serviços especializados, devendo serem salvaguardas as cláusulas que assegurem o cumprimento do RGPD por parte desses prestadores de serviços (Anexos – Mod.2).

2.3. BOAS PRÁTICAS NA IMPLEMENTAÇÃO DO RGPD EM EMPRESAS DO CANAL HORECA

A implementação do RGPD implica, para além do domínio sobre o negócio, um claro conhecimento do próprio regulamento, bem como do ecossistema tecnológico envolvente, para o que se sugere a aplicação de 6 princípios:

1. **Disseminação de uma Cultura de Proteção de Dados** – criação de uma cultura de respeito e consideração pelos direitos dos titulares dos dados e de valorização da cadeia de valor digital, designadamente na criação de novos produtos/serviços e seus impactos no modelo de negócios. Assim, os hotéis, hostels, restaurantes, ou outros estabelecimentos similares, deverão passar a sensibilizar os seus diversos colaboradores para o facto de que os dados sobre clientes pertencem aos próprios, devendo estes ter conhecimento sobre a natureza dos mesmos e sobre as finalidades do tratamento a ser efetuado, solicitando a sua prévia autorização. Esta nova realidade, em vez de sobressair com uma contrariedade, deve ser cultivada no sentido da valorização da relação com os clientes e no aumento da confiança dos mesmos, sobre os serviços prestados;
2. **Auditoria aos fluxos de recolha e tratamento de dados existentes** – as empresas do canal HORECA, a exemplo da generalidade das empresas, possuem inúmeras

estruturas de dados espalhadas por diversos computadores, bem como em diferentes suportes (Ex: Folhas de cálculos e/ou aplicações de suporte às operações e de natureza produtiva). O levantamento e sistematização da realidade existente e o redesenho dessas estruturas e seus suportes, designadamente em termos de integração dos dados, é fundamental para garantir a pseudonimização e encriptação dos mesmos, bem como de reserva de acesso a utilizadores qualificados. Para o efeito deverão os hotéis, hostels, restaurantes, ou outros, desenvolver essas ações, seja através de recursos próprios, ou por via da subcontratação desses serviços. Nessa circunstância deverão acautelar que os subcontratantes cumprem com as obrigações decorrentes do RGP, designadamente em termos da integridade, confidencialidade e preservação dos dados e da identidade dos respetivos titulares dos mesmos;

3. **Elaboração de procedimentos documentados para a recolha e tratamento de dados** – o RGPD obriga que se faça prova efetiva de que se cumpre com as especificidades do mesmo, pelo que a criação de processos devidamente documentados é vital (*acountability*);
4. **Avaliação do grau de conformidade *(compliance)* de partes contratadas** – a verificação, análise e garantia de que entidades com quem se tenham contratos de fornecimento de serviços é crítica para garantir a necessária conformidade com o RGPD. Alguns exemplos dessas situações são as empresas fornecedoras de *cloud services* e de SaaS *(software as a service)*, pelo que deverão as empresas do canal HORECA estabelecer os necessários acordos / contratos com a inclusão de cláusulas específicas;
5. **Monitorização dos processos instalados *(breach procedures)*** – uma medida de segurança muito importante prende-se com a monitorização, controlo e correção permanentes de falhas no tratamento de dados, mitigando a sua ocorrência e a consequente obrigação de notificação para as entidades competentes, com o risco das penalizações daí advindas;
6. **Acompanhamento e *feedback* aos titulares de dados** – a necessidade de saber, em cada momento, se um determinado titular de dados solicitou uma retificação, a portabilidade dos seus dados ou ainda se invocou o "direito a ser esquecido", implica a existência de mecanismos/processos para a recolha dessa informação, permitindo reagir e atuar em conformidade, num *timing* ajustado.

CASOS PRÁTICOS

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

3. A ADOÇÃO DO RGPD NOS ASSOCIADOS DA AHRESP – CASOS PRÁTICOS

A Associação da Hotelaria Restauração e Similares de Portugal (AHRESP) nasceu em 1896. Atualmente, é a maior associação empresarial na defesa e representação de um setor que é uma das mais importantes locomotivas do desenvolvimento e da economia da sociedade portuguesa: o **Turismo**.

A AHRESP representa um diversificado conjunto de empresas dos setores da restauração e bebidas e do alojamento turístico, compreendo o universo dos seus associados cerca de 4% do total de empresas existentes em Portugal no Canal HORECA. Considerando os dois grandes grupos em que se subdividem os seus associados, atentemos no universo e diversidade das atividades representadas:

I. **Área Restauração**
   a) Restauração – inclui os restaurantes tradicionais, típicos, de fado, casas de pasto, auto-serviços, e estabelecimentos equiparados;
   b) Pastelarias e cafés – inclui as pastelarias com fabrico próprio, padarias, confeitarias, leitarias, cafés, cafetarias, casas de chá, geladarias e estabelecimentos equiparados;
   c) Indústria, comércio alimentar e emissores de vales de refeições – inclui a indústria/comércio alimentar e de bebidas e as empresas emissoras de vales de refeições;
   d) Animação turística – inclui os casinos, bingos, e outros espaços de jogo, espaços de animação turística, empresas de organização de eventos, bares, discotecas e estabelecimentos de animação equiparados;
   e) Restauração coletiva – inclui os concessionários de restauração e alimentação coletiva, cantinas, refeitórios e fábricas de refeições;
   f) Restauração de serviço rápido – inclui os restaurantes de serviço rápido, serviços de restauração ao domicílio e outros equiparados.

II. **Alojamento**
   a) Empreendimentos turísticos e alojamento local – inclui os estabelecimentos hoteleiros, aldeamentos, apartamentos e conjuntos turísticos, turismo de habitação, turismo em espaço rural e de natureza, hostels, outros estabelecimentos de alojamento local, e outros equiparados;
   b) Hotelaria de ar livre – inclui o campismo, caravanismo, hotelaria de ar livre e parques temáticos.

Assim, compreendendo uma diversidade de associados significativa, não só pela dispersão das atividades, mas também pela dimensão das estruturas organizativas associadas, optou-se por fazer a análise das especificidades na aplicação do RGPD, bem como da construção de casos práticos, em resultado das complexidades associadas, sendo estas transversais ao universo de empresas.

3.1. CHECK-LIST

A *check-list* que se apresenta, sintetiza as principais atividades a partir das quais se podem colocar algumas dúvidas sobre as complexidades associadas ao cumprimento do RGPD. Foram considerados 3 níveis, os quais decorrem da agregação das atividades, não estando estas

dependentes do tipo de atividade e sendo por isso transversais a diferentes Associados da **AHRESP**:

- **Nível 1** – reproduz a realidade das unidades de negócio que não fazem uso de dados pessoais, enquanto elementos de suporte ao negócio, não deixando de "recolher" dados sobre clientes, em resultados dos pagamentos efetuados através do sistema POS, assim como possui informação sobre os seus trabalhadores, inerente às suas responsabilidades em termos de pagamento de salários e demais obrigações legais;
- **Nível 2** – reproduz a realidade das unidades de negócio que, para além das ações anteriores, já recolhem dados com vista a perceber a recetividades da sua oferta junto de clientes, podendo ainda ter algumas ações complementares em que registam dados que permitam a identificação de clientes;
- **Nível 3** – reproduz a realidade das unidades de negócio que, para além das ações descritas no Nível, podendo incluir todas ou em parte das descritas no Nível 2, se diferenciam das anteriores porque possuem uma estratégia clara para o uso do digital, potenciando o contacto e a lealdade junto dos seus clientes.

Ações com impacto possível ao nível do tratamento de dados pessoais		Nível 1 (Baixa complexidade)	Nível 2 (Moderada complexidade)	Nível 3 (Alta complexidade)
Emissão de faturas (POS)		✓		
Processamento de dados sobre o Pessoal (interno vs externo)		✓	✓	
Controlo de ponto com recolha de dados (interno vs externo)		✓	✓	
Vídeo vigilância (controlo e segurança das instalações)				✓
Site sem *cookies*		✓		
Ações de Marketing Digital	Online Marketing (cookies, SEO, …)		✓	
	e-mail Marketing		✓	✓
	Contextual Marketing			✓
	Social Media Marketing		✓	✓
	Facebook Ads e Google Adwords		✓	
	Mobile Marketing (envio de SMS)		✓	✓
	Mobile Marketing (uso de Apps)			✓
	Uso de Captive Portals (wireless)			✓
	Outras ferramentas digitais			✓
Uso de aplicações de gestão de clientes (CRM)				✓
Criação e manutenção de Banco de Conteúdos próprio				✓

3.2. CASOS PRÁTICOS

Vejamos 3 casos práticos, idealizados por forma a reproduzirem situações reais:

3.2.1. Caso "Pastealria Silva" (Nível 1)

Descrição do caso:

A "Pastelaria Silva", é um pequeno estabelecimento situado numa rua movimentada em Setúbal com diverso comércio local e alguns escritórios por perto. Sem possuir fabrico próprio de bolos e pão, a "Pastelaria Silva" aceita, no entanto, encomendas de bolos de aniversário cuja confeção fica a cargo do fornecedor que diariamente os abastece. Por outro lado, para além do serviço normal de pastelaria/cafetaria, a "Pastelaria Silva" serve refeições ligeiras, compostas por sopa, saladas, salgados e sandes.

A “Pastelaria Silva” tem como trabalhadores, o sr. Silva, empresário em nome individual e proprietário da mesmo, a sua esposa, que assegura o serviço de cozinha e dois empregados. Idêntico a milhares de outros estabelecimentos existentes no país, tem um sistema de PoS (*Point of Sale*), que inclui pagamento através da Rede MB.

O sr. Silva recorre a uma empresa de contabilidade que lhe garante o cumprimento das suas obrigações fiscais, bem como o pagamento de salários. Influenciado por clientes e filhos, começa a pensar em fazer qualquer coisa *online*, porque lhe dizem que “é bom para o negócio”.

Questões do RGPD e respostas:

- O sr. Silva está preocupado com o RGPD porque lhe referiram que se os clientes pedirem que inclua o nome na fatura isso traz-lhes outras responsabilidades, por causa do RGPD. O que deverá fazer?
    - Na verdade, a “Pastelaria Silva” e o sr. Silva, enquanto “responsável” pelo tratamento de dados, não deve ter preocupações acrescidas uma vez que o seu negócio não acarreta responsabilidades específicas, em termos de RGPD. Isto porque a que emissão de faturas não tem associado nenhum tratamento dos dados pessoais dos clientes, para além dessa mesma finalidade. Nesse sentido tudo continua a ser como anteriormente ao RGPD;
    - Do ponto de vista da análise específica, o facto das faturas terem o número fiscal do cliente já por si só é identificativo do mesmo, independentemente de constar também o seu nome;
    - No entanto, atendendo a que o sr. Silva recorre a um sistema PoS através de um fornecedor específico, bem como a um TOC para a prestação de serviços de contabilidade, deverá garantir que não existe qualquer tratamento sobre os dados pessoais referentes aos seus clientes, por esses fornecedores, para além do confinado à emissão das faturas respetivas e demais obrigações legais. Para o efeito deverá solicitar que esses fornecedores lhe entreguem uma Declaração nesse sentido, a qual poderá seguir o modelo apresentado (Anexos – Mod.2).
- Um cliente mais sensível às questões relacionadas com a proteção dos dados pessoais, questionou-o sobre a informação que lhe deu para confeção do bolo de aniversário do seu filho. Para confeção do bolo de aniversário, o sr. Silva costuma pedir o nome do aniversariante, a data do aniversário e a idade. Dados estes que são normalmente recolhidos em qualquer situação semelhante. A prática do sr. Silva é tomar nota desses dados no talão de encomenda do bolo, o qual é feito em triplicado: i) original para o cliente; ii) duplicado para o fornecedor que vai confecionar o bolo; iii) triplicado para controlo da pastelaria. Como deverá passar a funcionar o sr. Silva, considerando ainda a eventualidade da morada do cliente também ficar registada, o que já tem acontecido para entrega do bolo e das respetivas velas no domicílio?
    - É uma situação que merece ser devidamente acautelada no âmbito do RGPD, uma vez que, efetivamente, se constitui como um ato de recolha de dados pessoais com o risco dos mesmos poderem ser alvo de tratamento específico, desde logo por via de entidades terceiras;
    - Apesar do sr. Silva se limitar ao simples registo desses dados para os fins visados, sem qualquer outro tipo de intervenção, e eliminando-os quando

termina o bloco de papel onde regista essas encomendas, deverá assegurar que o seu fornecedor cumpre com esses mesmos princípios e que, para além do mais, não os cede a outras entidades;

- Assim, deverá proceder de duas formas:
  - Relativamente aos clientes – informá-los de que os dados recolhidos serão partilhados com quem irá confecionar o bolo e solicitar-lhes, por escrito, autorização para o efeito. Deverá igualmente assegurar que os dados recolhidos serão exclusivamente utilizados para os fins visados e que os mesmos serão imediatamente eliminados após essa utilização;
  - Relativamente ao seu fornecedor de bolos – assegurar que o mesmo não faça outra utilização desses dados do que aquela que é exclusivamente necessária para a confeção de cada bolo, eliminando-os após, bem como que os mesmos não venham a ser partilhados com outras entidades. Para o efeito deverá ser subscrito um Acordo de Proteção de Dados conforme proposto (Anexos – Mod.2).

- O sr. Silva está preocupado com o RGPD, uma vez que lhe disseram que deve manter privada a informação sobre os seus trabalhadores. O que deverá fazer?
  - Não estando obrigado a implementar o RGDP, em termos da definição de uma política e de mecanismos técnicos e/ou organizacionais, o sr. Silva, no entanto, deverá estar sensível à criação de novos hábitos na relação com dados sobre os seus trabalhadores:
    - Assim, caso efetuasse internamente o respetivo processamento de salários, bem como demais obrigações fiscais da firma, deveria assegurar-se que o acesso aos dados sobre os trabalhadores era apenas efetuado por pessoa(s) autorizada(s) e que não era feito qualquer outro tipo de uso da informação subjacente, para além do necessário;
    - Sendo o processamento de salários realizado externamente por TOC, o sr. Silva deverá subscrever com o mesmo um contrato (Anexos – Mod. 2), ou obter da parte dele uma declaração, em que, na qualidade de subcontratante, se compromete a cumprir com o RGPD, através de medidas técnicas e organizativos sobre a sua (dele) responsabilidade;
    - Em qualquer dos casos, deverá ter em consideração que, se a natureza dos dados recolhidos for para além daqueles que são obrigatórios para a gestão administrativa de salários, férias e outras obrigações, designadamente fiscais e perante os regimes de segurança social, poderá ter de dar conhecimento prévio aos seus colaboradores/funcionários sobre a natureza dos dados recolhidos e suas finalidades, estando esses sujeitos à aprovação prévia dos respetivos titulares. Esta condição é particularmente relevante sempre que estiverem associados dados que pela sua natureza possam ser considerados sensíveis (1.2).

3.2.2. Caso “Discoteca Bom Som” (Nível 2)

Descrição do caso:

A “Discoteca Bom Som”, localizada em Ponta Delgada, tem vindo a implementar um conjunto de medidas com vista ao aprofundamento do contacto com os seus clientes, atendendo a que uma parte dos mesmos são clientes regulares, em particular os que sempre que visitam a ilha fazem questão de voltar, ou então são clientes novos que vêm por sugestão de amigos e familiares que já lá estiveram antes, designadamente estrangeiros. Sendo uma empresa de animação noturna, a sociedade é detida por um jovem casal de açorianos que tem vindo a investir no setor do Turismo.

A “Discoteca Bom Som”, tem um quadro de 8 colaboradores, entre pessoal que faz o atendimento ao balcão, DJ’s e seguranças/porteiros, recorrendo a um TOC que lhes faz o processamento de salários, demais obrigações fiscais e perante a segurança social. Os sócios não são remunerados.

A discoteca faz uso de estratégias de Marketing Digital, tendo um *site* otimizado com SEO, fazendo uso de *cookies* e recorrendo a *Adwords*, soluções través das quais potencia a sua oferta junto daqueles que pesquisem por animação noturna na ilha. Por outro lado, tem uma rede de seguidores no Facebook que lhes permite anunciar eventos em datas especiais, facilitando a publicação de fotos pelos seus frequentadores. Mais recentemente implementou um *captive portal* onde recolhe diversa informação sobre os clientes, a partir da oferta de acesso à Internet que é disponibilizada num espaço interior mais tranquilo. Com fundamento na informação recolhida, a qual gera uma base de dados específica, pretende lançar campanhas junto de clientes, personalizando-as de acordo com a regularidade com que visitam a discoteca ou participam em eventos específicos.

Apesar de não terem um tratamento centralizado de toda a informação relacionada com clientes (não possuem um CRM – Customer Relationship Management), fazem tratamento de dados recolhidos por diversas fontes, tentando otimizar a relação com os seus clientes e o contacto por via dos meios digitais.

Questões do RGPD e respostas:

- Quais as preocupações que a empresa deve ter no plano dos dados pessoais associados às faturas dos seus clientes?
    - As preocupações devem ser semelhantes às do caso referido no Nível 1 (Pastelaria Silva), desde logo porque recorrendo a um sistema POS através de um fornecedor específico, bem como a um TOC para a prestação de serviços de contabilidade, deverá garantir que não existe qualquer tratamento sobre os dados pessoais referentes aos seus clientes, para além do confinado à emissão das faturas respetivas e demais obrigações legais. Para o efeito deverá solicitar que esses fornecedores lhe entreguem uma Declaração nesse sentido, podendo optar pelo estabelecimento de um Acordo de Proteção de Dados conforme proposto (Anexos – Mod.2).
- E quais devem ser as preocupações relacionadas com os dados pessoais associados aos seus colaboradores?
    - Importa esclarecer que as responsabilidades sobre o tratamento dos dados pessoais referentes aos trabalhadores, sendo necessária para efeitos do processamento de salários e demais obrigações, apenas pode ser mais complexa e exigente, em termos da conformidade com o RGPD, dependendo da natureza dos dados recolhidos, independentemente desses

colaboradores/funcionários serem efetivos ou eventuais. Assim, há que ter em consideração se os dados recolhidos são apenas os necessários para as obrigações "normais", ou se incluem outras categorias, designadamente dados considerados sensíveis (1.2), o que implicaria que os colaboradores/funcionários tivessem conhecimento sobre os mesmos, sendo necessária a sua autorização prévia;
    - No essencial mantém-se o conjunto de orientações referidas no caso anterior, no qual, sendo o processamento de salários realizado, deverá ser estabelecido contrato, ou obter declaração, em que, na qualidade de subcontratante, essa empresa se compromete a cumprir com as determinações do RGPD, através de medidas técnicas e organizativos sobre a sua (deles) responsabilidade (Anexos – Mod.2).
- Deve a empresa registar o tratamento de dados pessoais que efetua?
    - Atendendo a que a empresa tem uma ação consciente e regular, relacionada com o tratamento de dados pessoais, malgrado ter menos de 250 trabalhadores, deverá implementar o RGPD e garantir a existência de mecanismos técnicos e operacionais de registo e controlo dos respetivos atos relacionados com o tratamento de dados.
- E deve pedir autorização prévia aos seus clientes para poder enviar-lhes SMS ou e-mails com campanhas e promoções específicas dirigidas aos mesmos (Ex: Descontos no dia de aniversário)?
    - Claro que sim! A empresa, na qualidade de responsável pelo tratamento de dados, bem como as entidades por si subcontratadas com essa ação correlacionada, devem informar os (potenciais) clientes (titulares de dados) das intenções subjacentes à recolha dos dados, bem como do período em que preveem usá-los, assim como se pretendem partilhá-los com terceiros, solicitando consentimento prévio aos mesmos. Deverá criar as condições para que os titulares de dados possam autorizar o uso parcial ou total dos mesmos, obtendo da parte desses o prévio consentimento para o efeito, através de assinatura de declaração específica (Anexos – Mod.1);
    - Deverá ainda assegurar os necessários mecanismos tecnológicos que melhor garantam a segurança dos dados, prevenindo quaisquer situações de violação dos mesmos, ou de uso indevido. Para este efeito deverá igualmente prevenir a existência de procedimentos de acesso condicionado a determinados utilizadores, com permissões específicas em função das necessidades e responsabilidade de cada um dentro da empresa (Ex: Gestor das Redes Sociais), bem como de pseudonimização e/ou cifragem dos dados, em situações específicas como seja as que se prendem com dados sensíveis.
- Deverá a empresa nomear um Encarregado pela Proteção de Dados (EPD)?
    - Dependendo da tipologia de dados pessoais recolhidos, em particular se os mesmos podem ser considerados sensíveis, bem como da "intensidade" e regularidade da recolha poderá ser necessário nomear um EPD, ou um subcontratante que assuma as responsabilidades inerentes;
    - Mesmo que a empresa não recolha dados massivamente, nem registe dados de natureza sensível, será recomendável, na circunstância, a nomeação de um EPD, ou subcontratante com essas responsabilidades, o qual deverá

garantir a existência e controlo dos mecanismos técnicos e organizacionais associados, por forma a que, desde logo, possa fazer face a qualquer pedido de informação por parte da CNPD ou de entidades do Estado, tanto em termos nacionais, como no espaço da UE.

3.2.3. Caso “Aldeamento Sol, Mar e Ar Puro” (Nível 3)

Descrição do caso:

O ”Aldeamento Sol, Mar e Ar Puro”, localizado na Lourinhã, compreendendo uma área de 12 ha, é constituído por um conjunto de unidades de alojamento e de lazer, bem como de espaços de restauração com uma oferta diferenciada na região de Lisboa, situando-se dentro de uma vasta propriedade de produção de fruta e vitivinícola.

Tendo começado por ser uma solução de turismo inserido em espaço rural, através de um conjunto de 6 pequenas habitações, o “Aldeamento Sol, Mar e Ar Puro” é muito procurado por pessoas de idade mais avançada (seniores), tanto nacionais como estrangeiros, tendo em conta a sua oferta específica em termos de saúde e bem-estar, para além de um golfe de 9 buracos.

Sendo detido por um Grupo com outros investimentos no setor do Turismo, a sociedade (SA), conta com 350 trabalhadores espalhados pelas regiões de Lisboa e Setúbal, onde se centram as suas principais ofertas. Na capital, o Grupo tem vindo a potenciar a oferta de alojamento em *hostels*, potenciando uma oferta turística dirigida a jovens estrangeiros em visita à cidade (*City Short Breaks*).

No caso do ”Aldeamento Sol, Mar e Ar Puro”, em face da oferta ser muito direcionada para o Turismo Sénior, com serviços muito diversificados em termos do mercado de Saúde e Bem-Estar, a sociedade tem protocolos estabelecidos com clínicas e centros de reabilitação, entre outros, com vista a complementar os seus serviços diretos, proporcionando estadias longas de recuperação.

A sociedade tem uma estratégia clara e definida em termos de Marketing Digital, possuindo meios próprios para a conceber e implementar, através do recurso a empresas nas áreas dos sistemas e tecnologias de informação, as quais subcontrata, bem como com recurso interno a plataformas específicas (Ex: CRM, *Business Analysis*). Talvez devido ao facto de que os idosos em Portugal terem ainda reduzidos níveis de utilização de meios digitais, o “Aldeamento Sol, Mar e Ar Puro” é fundamentalmente procurado por turistas provenientes do norte da europa, os quais utilizam a Internet e fazem uso de aplicações digitais de modo mais regular. Esta realidade, consubstanciando a estratégia de alcançar mercados estrangeiros (Inbound Tourism), fez com que, desde há 3 anos que a sociedade tenha implementado uma app que permite aos seus clientes seguirem programas de recuperação personalizados, podendo aceder em permanência, por essa via, a todo o histórico do seu percurso, bem como a dados diversos sobre a sua saúde.

A sociedade detentora do “Aldeamento Sol, Mar e Ar Puro”, efetua autonomamente, com recurso a pessoas e meios tecnológicos internos, todas as atividades de gestão correntes e necessárias aos seus negócios, onde se inclui, designadamente, a Gestão dos Recursos Humanos e todas as tarefas de natureza administrativa associadas, como sejam as relativas ao processamento de salários, férias e demais obrigações com o Estado.

Questões do RGPD e respostas:

- Quais as preocupações que a empresa deve ter no plano do tratamento de dados pessoais com os seus clientes?
    - Sendo uma empresa em que é inequívoca a obrigatoriedade de implementação do RGPD, a empresa deve cumprir com todos os requisitos do mesmo, começando por fazer um levantamento da realidade existente, a partir das bases de dados existentes e da informação nelas contidas, bem como deve projetar as soluções futuras que salvaguardem os direitos dos titulares de dados;
    - Deverá informar todos os seus clientes da natureza dos dados a serem recolhidos, bem como da finalidade dos mesmos, submetendo ao seu prévio consentimento (Anexos – Mod.1);
    - É igualmente obrigada a designar um Encarregado pela Proteção de Dados (EPD), o qual deverá desenhar os processos e estabelecer os respetivos procedimentos, seja por iniciativa própria, seja em articulação com entidade(s) externa(s). Esta obrigatoriedade decorre da circunstância de que muitos dos dados pessoais serem de natureza sensível, uma vez que se prendem com a saúde dos seus clientes. A empresa poderá subcontratar o serviço, não deixando de ter um responsável interno sobre o tratamento de dados que deverá articular com o subcontratante e garantir a efetivação de todas as medidas;
    - Deverá implicar nesse processo de garantia de direitos e de segurança de dados, as entidades com quem tem protocolos estabelecidos atendendo a que existe a partilha de dados sensíveis, estabelecendo acordos de salvaguarda das suas responsabilidades e de conformidade dos mesmos com as obrigações do RGPD (Anexos – Mod.2);
    - Da mesma forma deve garantir todos os mecanismos de segurança e de limitação de acesso a esses dados, quer por defeito, quer pelas soluções tecnológicas, obtendo da parte das empresas a que tenha de recorrer para a prestação desses serviços, as necessárias garantias.
- Fruto das especificidades da atividade, em termos de oferta de alojamento para fins turísticos, tanto no caso do aldeamento na Lourinhã, como nos *hostels* em Lisboa, a sociedade tem de ter em consideração e cumprir com o regime jurídico[4] de entrada, permanência, saída e afastamento de estrangeiros do território nacional, o qual refere que "*As empresas exploradoras de estabelecimentos hoteleiros, meios complementares de alojamento turístico ou conjuntos turísticos, bem como todos aqueles que facultem, a título oneroso, alojamento a cidadãos não nacionais, são obrigados a comunicá-lo, no prazo de três dias úteis, por meio de boletim de alojamento ao Serviço de Estrangeiros e Fronteiras (SEF)*". Essa informação, prestada por via do preenchimento do Boletim de Alojamento e contendo (necessariamente) dados pessoais, é efetuada através da plataforma eletrónica SIBA - Sistema de Informação dos Boletins de Alojamento[5].
    - Por outro lado, a sociedade deve ter em consideração que, sendo a solicitação do Cartão de Cidadão uma prática frequente nos estabelecimentos

[4] https://siba.sef.pt/legislacao-e-protocolos/
[5] https://siba.sef.pt/

de alojamento, por vezes reproduzindo-o mesmo (Ex: Digitalização, fotocópia), esta é interdita por lei[6], seja através fotocópia ou por qualquer outro meio sem o consentimento do titular, salvo nos casos expressamente previstos na lei ou mediante decisão de autoridade judiciária. Assim, a sociedade deverá solicitar consentimento expresso e inequívoco por parte do respetivo titular de cada Cartão de Cidadão[7], o qual deverá assinar documento específico nesse sentido.

- A sociedade recolhe regularmente depoimentos de clientes, bem como realiza registos em imagem dos mesmos, que usa para comprovar a eficácia dos seus processos e da qualidade da sua oferta de serviços. Deverá ter alguma preocupação especial com este facto?
    - Sim. Deverá garantir o consentimento prévio dos próprios titulares desses dados, designadamente sobre a sua disponibilidade para participarem nas sessões de vídeo / fotografias a serem realizadas, informando sobre os fins e limites de utilização, designadamente em termos do "tempo de vida" desses conteúdos (digitais).
- Que preocupações específicas deverá ter a sociedade com os dados pessoais relativos aos seus funcionários?
    - Deve assegurar-se que o acesso aos dados sobre os trabalhadores seja apenas efetuado por pessoa(s) autorizada(s), às quais lhe sejam cometidas responsabilidades específicas no âmbito da gestão administrativa do pessoal e das obrigações legais a serem cumpridas nesse âmbito, tendo ainda em consideração as medidas técnicas e organizativos necessárias, as quais garantam a integridade, confidencialidade e acesso dos trabalhadores aos respetivos dados de que são titulares;
    - Deverá ainda de ter em consideração que, se a natureza dos dados recolhidos for para além daqueles que são obrigatórios, poderá ter de dar conhecimento prévio aos seus colaboradores/funcionários sobre a natureza dos mesmos e suas finalidades, estando sujeitos à aprovação prévia dos respetivos titulares. Esta condição é particularmente relevante sempre que estiverem associados dados que pela sua natureza possam ser considerados sensíveis (1.2). A exemplo da situação anterior, deverá igualmente dotar-se dos mecanismos técnicos e organizativos que garantam a integridade, confidencialidade e acesso dos trabalhadores aos respetivos dados de que são titulares.

[6] https://dre.pt/home/-/dre/107114304/details/maximized
[7] http://bit.ly/2xfImPS

RECOMEMNDAÇÕES FINAIS

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

4. RECOMENDAÇÕES FINAIS E CONTACTOS

4.1. RECOMENDAÇÕES FINAIS

Em conclusão, apresenta-se uma lista de recomendações que as empresas nos setores da restauração e bebidas e do alojamento turístico, devem ter presente relativamente à adoção do RGPD:

- O RGPD convida à reflexão sobre o uso de dados, em particular de dados pessoais, com utilidade para a criação de fatores de sustentabilidade e competitividade nos negócios. Hoje, a Transformação Digital em curso, desafia as empresas e os empresários a potenciarem novas soluções em que a Inovação e Criação de Valor, por via do digital, se assumem como pilares do maior relevo;
- A adoção do RGPD implica a criação de novos hábitos e de uma nova cultura, transversal às organizações, em que o respeito pela privacidade e a vontade dos titulares de dados, deverá fazer parte integrante da cadeia de valor. Nesse sentido as empresas devem passar a solicitar o consentimento prévio dos titulares de dados, sobre as suas ações de tratamento dos mesmos, devendo fazê-lo de forma esclarecedora e inequívoca;
- Sem prejuízo da criação de uma sensibilidade mais alinhada com as preocupações do RGPD, o mesmo só se aplica a empresas que tratem de dados pessoais de pessoas singulares para outros fins além de faturação (Ex: Envio de *newsletters* e outras ações de marketing). Todas as empresas que recolhem, armazenam ou tratam dados pessoais estão abrangidas pelo regulamento;
- A obrigatoriedade de manter um registo das atividades de tratamento de dados é apenas válida para empresas com mais de 250 trabalhadores, com exceção daquelas em que os direitos e liberdades do titular dos dados, não seja ocasional ou abranja categorias especiais de dados, as quais se encontram referidas nos Artº 9 e Artº 10º. As empresas com mais de 250 colaboradores são obrigadas a manter um registo de todas as atividades de tratamento, com as seguintes informações:
    - Nome e contactos do responsável pelo tratamento de dados;
    - Finalidades do tratamento;
    - Descrição das categorias de titulares e de dados pessoais;
    - Categoria de destinatários a quem os dados pessoais sejam divulgados;
    - Transferências de dados pessoais para outros países ou organizações internacionais, caso aplicável;
    - Prazos previstos para eliminar os dados, se possível;
    - Descrição geral das medidas técnicas e organizacionais para a segurança dos dados, se possível.
- O RGPD aplica-se a todas as empresas que tratem dados pessoais, independentemente do negócio ser orientado para B2C, ou para B2B. No caso da orientação ser B2B, devem ser analisadas as bases de dados existentes, verificando se existem dados pessoais, tendo em consideração que um email específico pode der determinante para identificar uma pessoa, bem como que, no caso dos empresários em nome individual, todos os dados acerca dos mesmos são potencialmente pessoais;
- A nomeação de um encarregado de proteção de dados só é obrigatória nos seguintes casos: autoridades e organismos públicos; organizações que giram dados sensíveis em larga escala; ou organizações que exijam controlo regular e sistemático dos titulares dos dados;

- As empresas que possuíam históricos de dados pessoais, antes de 25 de maio de 2018, data a partir da qual começou a vigorar o RGPD, deverão fazer o inventário desses mesmos dados e tomar as medidas adequadas, de acordo com o regulamento. Poderão essas empresas ter de solicitar consentimento aos titulares desses dados já na sua posse ou, em última instância, apagar os mesmos (exceto se tiverem uma implicação legal, como é o caso do NIF para efeitos de faturação);
- Nas situações em que os clientes solicitem uma intervenção específica sobre os seus dados, as empresas deverão proceder em conformidade, num prazo de tempo considerado razoável, enquanto o "direito a ser esquecido" deve ser feito *sem demora injustificada*. Sublinha-se que o "direito a ser esquecido" não implica a eliminação do histórico quando estão em causa obrigações legais e tempos associados, como seja as faturas antes emitidas;
- O exercício do direito de acesso, retificação, cancelamento e omissão, por parte do titular de dados, pode se sobre a totalidade dos dados ou apenas em parte, devendo a empresa agir em conformidade;
- Os princípios do RGPD também se aplicam ao conjunto dos trabalhadores, desde logo quando se recolhem outros dados para além dos estritamente necessários para efeitos do estabelecimento da relação contratual e respetivas obrigações legais, para o que se deve obter o consentimento prévio do trabalhador e/ou candidato a emprego;
- As empresas devem estabelecer com os seus fornecedores cláusulas de (co)responsabilidade sempre que se verifique qualquer acesso e/ou partilha de dados, salvaguardando as responsabilidades de cada parte no tratamento dos mesmos e da existência dos respetivos consentimentos dos titulares, para o efeito;
- Sempre que se verifique uma quebra de segurança com impacto ao nível da violação de dados pessoais, as empresas são obrigadas a notificar a autoridade de supervisão nacional (CNPD), o que deverá ocorrer num prazo máximo de 72h. Concomitantemente, quando a violação for suscetível de acarretar um risco elevado para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunicará a violação dos dados pessoais à pessoa em causa, excetuando os casos em que, pelas medidas técnicas e organizativas adotadas, os mesmos sejam indecifráveis (encriptação), ou sejam tomadas medias subsequentes que mitiguem/anulem o risco elevado para os direitos e liberdades das pessoas. Nos casos em que a comunicação direta, junto do titular de direitos, implicaria um esforço desproporcionado, haverá, em vez disso, uma comunicação pública ou outra medida análoga, segundo a qual as pessoas em causa possam ser informadas de forma igualmente eficaz.

4.2. INFORMAÇÕES COMPLEMENTARES

Poderão ainda os associados da AHRESP consultar informação complementar sobre a aplicação do RGPD, tendo em consideração a especificidade de cada realidade organizacional, nos seguintes sítios da Internet:

- **Regulamento Geral de Proteção de Dados** (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT)
- **Comissão Europeia (CE)**
    - Reforma das regras de proteção de dados da UE (https://ec.europa.eu/info/law/law-topic/data-protection/reform_pt?pk_source=google_ads&pk_medium=paid&pk_campaign=gdpr2167);

    - Regras para empresa e organizações (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_pt);
    - Data protection - Better rules for small business (https://ec.europa.eu/justice/smedataprotect/index_en.htm)
- **Comissão Nacional de Proteção de Dados (CNPD)** – Espaço RGPD (https://www.cnpd.pt/bin/rgpd/rgpd.htm);
- **Turismo de Portugal** – Regulamento Geral Sobre a Proteção de Dados (http://www.turismodeportugal.pt/pt/quem_somos/Gest%C3%A3o/Informa%C3%A7ao_Gestao/Paginas/regulamento-geral-sobre-a-Protecao-de-dados.aspx)
- **IAPMEI** – Regulamento Geral Sobre a Proteção de Dados (https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Assistencia-Tecnica-e-Formacao/Regime-Geral-de-Protecao-de-Dados.aspx);
- **Diagnósticos / quizs** – existem diversas soluções que permitem fazer um diagnóstico *online* que esclarece sobre as necessidades específicas de cada organização. Para o efeito poderá inserir nos motores de busca a expressão "quiz rgpd".

4.3. CONTACTOS

Em caso de esclarecimentos complementares poderão ser contactados os serviços da ARHESP:

- Responsável pelo tratamento de dados: RGPD@ahresp.com
- Departamento Jurídico – Tel: 213 527 060 E-mail: ahresp@ahresp.com (Geral AHRESP)

ANEXOS

AHRESP
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

5. ANEXOS

Mod.1 – Declaração de consentimento para uso de dados pessoais

1. Identificação da entidade (responsável pela recolha e tratamento de dados pessoais)

Designação: (empresa HORECA)
Morada: …..
Telefone: …
e-mail do responsável pelo tratamento de dados: ……

2. Princípios da nossa Política de Privacidade de Dados

Desenvolvemos a nossa atividade com uma clara orientação para a satisfação dos nossos clientes, sendo assim relevante que procuremos, em cada momento, adequar os nossos serviços às necessidades e interesses dos mesmos, bem como às oportunidades que se vão desenhando no mercado onde nos inserimos.

Para que possamos continuar nesse sentido, necessitamos de recolher dados sobre os nossos clientes, os quais, cumprindo em primeiro com a necessidade de prestação de serviços que justificou a opção dos mesmos, potencia a criação de serviços ajustados que vão ao encontro dos seus interesses. Fazemo-lo de forma consciente e responsável, cumprindo com as determinações previstas no Regulamento Geral de Proteção de Dados (RGPD), assegurando a integridade, confidencialidade e acessibilidade dos dados pessoais que tratamos. Nesse sentido a nossa Política de Privacidade de Dados é estabelecida de acordo com o Regulamento UE n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Ao tomar conhecimento dos princípios e medidas associadas à recolha e tratamento dos seus dados pessoais, fica a conhecer as finalidades e especificidades do uso dos mesmos, estando habilitado a consentir que os mesmos possam ser por nós utilizados para esses fins, o que deverá explicitamente autorizar, através da sinalização das opções que lhe são apresentadas, assinando este documento.

3. Natureza e finalidade dos dados pessoais recolhidos

Os dados que recolhemos inscrevem-se em duas categorias[8]: i) Dados obrigatórios – situam-se neste âmbito todos aqueles que consideramos como fundamentais para a prestação dos nossos serviços; ii) Dados complementares – compreendem todos aqueles que consideramos como da maior relevância para a valorização da nossa oferta de serviços, permitindo conhecer os nossos clientes e as suas preferências.

4. Conservação dos dados pessoais recolhidos

Os dados pessoais recolhidos são conservados por um período de … anos, após a última data de fruição dos respetivos serviços, sendo destruídos após esse período, sem prejuízo da conservação dos mesmos por um período de tempo a que estejamos obrigados por imposição legal.

5. Partilha dos dados pessoais

A partilha dos dados pessoais de cada um dos nossos clientes é sujeita à aprovação prévia dos respetivos titulares.

ou

Os dados pessoais de cada um dos nossos clientes são partilhados dentro das empresas do grupo, sendo outras partilhas sujeitas à aprovação prévia dos respetivos titulares.

6. Direitos dos titulares de dados

[8] Os formulários / mecanismos de recolha de dados devem possibilitar ao cliente perceber qual a relação desses dados com as categorias mencionadas.

Os titulares de dados que pretendam exercer qualquer um dos seus direitos de acesso aos mesmos, retificação, portabilidade ou, dentro dos limites legais aplicáveis, limitação ou oposição ao tratamento, poderá em qualquer momento e mediante comunicação dirigida ao responsável pelo tratamento de dados, solicitando-o.

Poderá ainda o titular de dados solicitar que sejam apagadas quaisquer formas de registo existentes, bem como que lhe sejam facultados os seus dados através de meios que garantam a portabilidade dos respetivos dados.

7. Medidas técnicas e organizativas

Adotaremos as medidas técnicas e organizativas adequadas, e mais eficazes, para garantir a confidencialidade e integridade dos dados, evitando a sua perda, alteração e acesso ou difusão não autorizados.

8. Segurança e notificação

Os titulares de dados dispõem ainda do direito a serem informados sobre qualquer violação (ou potencial violação) sobre os seus dados pessoais, e de apresentar qualquer reclamação em matéria de violação de proteção de dados à Comissão Nacional de Proteção de Dados, cujos contactos se encontram disponíveis em www.cnpd.pt.

9. Responsável pelo tratamento de dados

Mais informações sobre a nossa Política de Privacidade e de Proteção de Dados Pessoais poderão ser solicitados para o nosso responsável pelo tratamento de dados, através do email: ……..

10. Consentimento / autorização

Autorizo que os meus dados pessoais sejam recolhidos e tratados para os fins seguintes:

☐ Figurar em Base de Dados de clientes, para efeitos de análise estatística e de caracterização dos interesses dos mesmos, por forma a poder gerar novos serviços ou a melhorar os existentes;

☐ Receber as nossas comunicações:

Para efeitos de conhecimento das atividades que desenvolvemos:

◯ Por e-mail ◯ Por SMS

Bem como para a divulgação de serviços e/ou de iniciativas/promoções consideradas como exclusivas dos clientes

◯ Por e-mail ◯ Por SMS

☐ Possibilitar a partilha de dados com entidades terceiras, as quais poderão vir a contactar-me para me darem a conhecer a sua oferta de produtos / serviços.

Nome: _____

Assinatura: _____ Data: _____ / _____ / _____

Mod.2 – Acordo de Proteção de Dados

(Este modelo de Acordo de Proteção de Dados deverá ser adaptado à especificidade da relação contratual a estabelecer entre as partes, designadamente quando o subcontratante assuma a responsabilidade pelo Tratamento de Dados, em representação da empresa HORECA).

1. Identificação da entidade (interessada no tratamento de dados pessoais)

Designação: (empresa HORECA)
Morada: …..
Telefone: …
e-mail do responsável pelo tratamento de dados: ……

2. Identificação do fornecedor (subcontratante)

Designação do subcontratante: ……..
Morada: …..
Telefone: …
Nome do responsável: ……
Contacto do responsável: ……

3. Declaração de princípio e âmbito do acordo

A (empresa HORECA), adota um conjunto de práticas visando a recolha e tratamento de dados pessoais, de acordo com as especificidades do Regulamento Geral de Proteção de Dados (RGPD), incluindo a responsabilização dos seus fornecedores nesse mesmo âmbito, em consonância com a sua prestação de serviços e/ou fornecimento de produtos, desde que as mesmas tenham uma qualquer relação com dados pessoais.

O subcontratante compromete-se a cumprir com a legislação existente sobre proteção de dados pessoais, designadamente com as especificidades que decorrem do RGPD, no que ao tratamento de dados pessoais possa estar relacionado com o âmbito dos seus serviços e/ou produtos.

O presente Acordo de Proteção de Dados (APD) estabelece, assim, as cláusulas a serem cumpridas pela subcontratante (…….), enquanto fornecedor da (empresa HORECA), considerando a observância e cumprimento específico do RGPD, em todas as suas determinações, pelo que deverá ser assinado por quem detenha poderes legais de representação da subcontratante.

4. Natureza do fornecimento de serviços e/ou produtos

O fornecimento de serviços e/ou produtos a serem realizados pelo(a) subcontratante (…….) à (empresa HORECA) sãos os seguintes: ……..

5. Garantias sobre o tratamento de dados

O subcontratante compromete-se a:

- Cumprir com as orientações sobre tratamento de dados emanadas da (empresa HORECA), considerando os dados pessoais relacionados com os seus clientes, bem como com os seus colaboradores/funcionários;
- A garantir que a transmissão de dados, incluindo as transferências de dados para países terceiros ou organizações internacionais, a ocorrer, só será permitida ao abrigo das disposições previstas no RGPD, e sempre sob autorização prévia da (empresa HORECA), salvaguardando as situações que seja obrigado a fazê-lo pelo direito da UE ou do Estado-Membro a que está sujeito, devendo, no entanto, informar dessa situação, antes de proceder a essa transferência, salvo se tal informação for proibida por motivos de interesse público;
- Assegurar a proteção dos dados pessoais a que possa ter acesso, designadamente no que à integridade e confidencialidade sobre os mesmos se refere, prevenindo qualquer forma de tratamento abusivo ou ilegal, bem como a sua perda, dano ou destruição acidentais;
- Garantir a implementação das medidas técnicas e organizacionais adequadas, das quais deverá poder fazer prova e/ou demonstração, designadamente em termos de acesso reservado aos mesmos;

- Assegurar o estabelecimento de acordos de confidencialidade com todos os seus colaboradores com acesso aos dados, fazendo prova da sua existência.

6. Garantias sobre os direitos dos titulares de dados

O subcontratante compromete-se a garantir a existência de medidas técnicas, designadamente de natureza tecnológica, como organizativas, designadamente em termos procedimentais, as quais sejam necessárias para responder aos pedidos dos titulares de dados, no âmbito dos seus direitos, com prontidão e nas condições previstas no RGPD (Artº 12º a Artº 22º).

7. Garantias sobre as medidas de segurança no tratamento de dados

O subcontratante compromete-se a garantir a existência de medidas técnicas, designadamente de natureza tecnológica, como organizativas, designadamente em termos procedimentais, conforme previsto no RGPD (Artº 32º), por forma a assegurar a proteção de dados desde a conceção e por defeito, a pseudonomização e a cifragem de dados pessoais nas situações consideradas necessárias, bem como a confidencialidade, integridade, disponibilidade e fiabilidade dos sistemas associados, em particular quando estiverem em causa categorias especiais de dados pessoais, como sejam os considerados sensíveis.

O subcontratante compromete-se ainda a garantir a existência de meios para a reposição atempada dos sistemas, em casos de ocorrência de avarias e/ou de outros incidentes, bem como da manutenção de todos os sistemas associados ao tratamento de dados e ainda a atualização dos mesmos, designadamente em termos de prevenção e resistência a ataques cibernéticos.

O subcontratante compromete-se a apagar ou a devolver todos os dados pessoais à empresa HORECA, depois de concluída a sua prestação de serviços, eliminando todas as cópias existentes, com exceção daquelas que possam eventualmente corresponder a necessidades conservação ao abrigo do direito da UE ou da legislação nacional.

8. Garantias sobre as obrigações de notificação e de comunicação na violação de dados

O subcontratante compromete-se a garantir a existência de medidas técnicas, designadamente de natureza tecnológica, como organizativas, designadamente em termos procedimentais, conforme previsto no RGPD (Artº 33º e Artº 34º), por forma a garantir a adequada assistência à empresa HORECA aquando da existência de violações sobre os dados e das suas obrigações perante a CNPD e/ou outras autoridades nacionais, bem como junto dos titulares dos respetivos dados.

9. Resolução do acordo em situações de incumprimento

Nas situações em que se verifique o incumprimento das obrigações previstas neste APD, ou em situações de negligência do subcontratante, designadamente por não-conformidade com os termos do RGPD, poderá a empresa HORECA de imediato rescindir o mesmo, bem como desenvolver as ações que considere adequadas, designadamente judiciais, com vista à mitigação das suas responsabilidades bem como de indemnização por eventuais prejuízos que esses atos lhe possam causar.

10. Contactos

Para efeitos de contacto entre as partes fica estabelecidos que serão usados no Ponto 1 deste APD.

Subcontratante: _____

Assinatura: _____ Data: _____ / _____ / _____


ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
AHRESP