Política de Privacidade

Enquadramento com Regulamento (UE) 2016/679 e Lei n.º 58/2019

Considerando a Lei n.º 58/2019 que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento 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 (RGPD), que veio substituir a diretiva 95/46/EC vertida para o ordenamento jurídico Português na Lei n.º 67/98 de 26 de Outubro.

Tendo em conta o paradigma de mundo orientado pela informação imediata e pelo poder dos dados pessoais colhidos e tratados com ou sem consentimento, ou pior, com ou sem conhecimento, estes normativos trazem algum do discernimento exigido a estas matérias, não deixando, no entanto, de acarretar mudanças de grande impacto, muitas delas fonte de forte controvérsia e com necessidade de maiores esclarecimentos.

Por esse motivo este documento apresentar-se-á de modo interpretativo, esclarecendo quanto às obrigações decorrentes desta Lei e a forma como a DAB as segue enquanto Controlador, ou seja, responsável pelo tratamento dos dados (parte II da PP) e Processador ou Subcontratado (Parte I da PP).

As alterações chave a saber começam, desde logo, pelo seu âmbito e pelos sujeitos a quem se destina, importando, por isso, começar por distinguir, de acordo com o artigo 4º do RGPD: Controlador(es)/Responsável(eis) pelo tratamento de dados e Processador/Subcontratante(es)

• ***Data Controller*** - (Controlador(es) ou Responsável(eis) pelo tratamento) – Será pessoa singular ou coletiva, ente público ou privado, agência, instituição ou qualquer outro organismo que decide como e porque é que os dados são processados. Portanto, pessoa física ou jurídica que, isoladamente ou em conjunto com outros, determina os fins e meios de processamento de dados pessoais.

Ora pelo artigo 5º do RGPD, o Controlador(es)/Responsável(eis) pelo tratamento é o responsável por provar o cumprimento dos princípios relativos ao tratamento de dados pessoais conforme está vinculado.

• ***Data Processor*** (Processador ou Subcontratante) - Será pessoa singular ou coletiva, ente público ou privado, agência, instituição ou qualquer outro organismo que trate os

dados pessoais por conta do responsável pelo tratamento destes (Subcontratante). Ou seja, aquele que processa dados pessoais em nome do(s) Controlador(es)/Responsável(eis) pelo tratamento.

Pelo artigo 28.º do RGPD, o tratamento pode ser efetuado em nome do(s) Controlador(es)/Responsável(eis) pelo tratamento, mas este é responsável por subcontratar apenas os Processadores/Subcontratantes que forneçam garantias suficientes de cumprimento do RGPD, isto é, Processador(es)/ Subcontratante(es) que tenham evidências da implementação das medidas técnicas e organizacionais adequadas, de tal forma que o processamento satisfaça os requisitos do regulamento.

Assim, todas as entidades da UE ou mesmo fora da UE, como Controlador(es)/Responsável(eis) pelo tratamento ou Processadores/Subcontratantes, devem implementar os controlos necessários para garantir a conformidade com o RGPD, Lei n.º 58/2019 em Portugal, desde que os dados a ser processados sejam

sobre cidadão da UE. Esta responsabilidade é partilhada entre o(s) Controlador(es)/Responsável(eis) pelo tratamento e Processador(es)/ Subcontratante(es), (as multas podem ser aplicadas a ambos).

Portanto, nos termos do RGPD/ Lei n.º 58/2019 a DAB é:

• Controlador/Responsável pelo tratamento de todos os dados que coleta dos seus clientes e, para prestação dos serviços subscritos e respetivo suporte (Parte II PP)

• Processador/Subcontratante enquanto agente de alojamento dos seus dados, registo de domínios ou venda de certificados *SSL* (Parte I PP)

PARTE I

Enquadramento e obrigações da DAB enquanto Processador ou Subcontratado

A - Informação e histórico

Passa a ser responsabilidade do(os) Controlador(es)/Responsável(eis) pelo tratamento de dados implementar medidas efetivas capazes de demonstrar a conformidade das atividades de processamento de dados, mesmo que, como já vimos, o processamento seja realizado por um Processador/Subcontratante de dados em nome do Controlador(es)/Responsável(eis) pelo tratamento, sendo que neste caso se

tratará de responsabilidade partilhada.

Então, o(s) Controlador(es)/Responsável(eis) pelo tratamento de dados passa(m) a ser o(s) responsável(eis) (eis) por garantir que os direitos assegurados pelo RGPD são efetivamente cumpridos, a saber os mais relevantes:

1 - Informação sobre os dados colhidos o seu fim e o consentimento

O pedido de consentimento para a colheita e processamento dos dados terá de ser levado a cabo de forma inteligível à vista do homem comum, contendo em si ou anexo qual o seu objetivo, fim ou fundamento. Portanto, o consentimento deve ser claro e distinguível de outros assuntos, facilmente acessível, fazendo uso de linguagem clara e simples. Permitindo ao titular dos dados, não só perceber o que está a consentir e quando o está a fazer, mas também do mesmo modo, ou com acesso e facilidade semelhantes, retirar o seu consentimento.

A todo o tempo o(s) Controlador(es)/Responsável(eis) pelo tratamento de dados deve (em) ter histórico de forma a poder provar que o consentimento foi adquirido de forma legítima e em conformidade com o RGPD.

Como Controlador(es)/Responsável(eis) pelo tratamento a DAB garante, ao dia de hoje, e na verdade desde sempre, que o consentimento da coleta dos dados do cliente subscritor, no ato do preenchimento da sua ficha de cliente, é obtido de maneira ativa e consciente. No entanto, e tendo em mente o princípio da clareza que o novo regulamento preconiza, por ação prática, a DAB passa a separar, desde logo, o consentimento à receção de informação generalizada da aceitação das cláusulas contratuais gerais, conforme disposto na parte II desta PP.

Como Processador/Subcontratado os dados que lhe são confiados são disponibilizados pelo Responsável pelo tratamento (cliente da DAB) tendo como fim ou objetivo que a DAB lhe preste o serviço contratado no ato da subscrição deste. No ato da subscrição do serviço, com eventual migração de dados e/ou a sua criação ou eliminação incremental, o Responsável pelo tratamento (cliente da DAB) entende e aceita que o objetivo final da sua ação é receber a prestação do serviço subscrito, conforme descrito na página *online* da DAB na data/hora em que o subscreveu. Para isso, na data/hora da sua subscrição ser-lhe-á enviado um email de confirmação, bem como no ato do pagamento e da ativação de

serviço. Todos estes emails ficarão guardados na área de cliente myDAB, acessíveis para consulta do Responsável pelo tratamento (cliente da DAB).

2 - Direito ao acesso

Um dos direitos que foram expandidos com o RGPD foi o direito de acesso dos sujeitos aos seus dados pessoais, à sua edição e retificação. Este direito estende a sua abrangência incluindo, agora, o direito de saber a todo o tempo se os seus dados estão ou não a ser processados, onde e para que finalidade. Além disso, o Controlador(es)/Responsável(eis) pelo tratamento deve viabilizar uma cópia dos dados pessoais, gratuitamente, e em formato exportável.

Como Controlador(es)/Responsável(eis) pelo tratamento de dados, a DAB viabiliza o acesso permanente aos dados, a todo tempo, por parte do seu titular e através da sua área reservada, este pode também alterá-los, salvaguardando sempre a correção destes dados. Por obrigações fiscais, tipicamente, quando os dados do cliente DAB se verificam como incongruentes, existe contacto proativo da nossa parte solicitando a correção. Poderá saber mais sobre o cumprimento desta obrigação na PARTE II desta PP.

Como Processador/Subcontratado a DAB não acede aos dados que lhe são confiados pelo Responsável pelo tratamento (cliente da DAB), salvo se, e apenas durante o tempo em que se afigure estritamente necessário para a prestação do serviço contratado. Desta feita, o acesso a estes dados estará a todo o tempo disponível e na esfera do cliente, através dos meios e dados enviados no ato da sua subscrição/ativação.

Poder-se-á dar o caso de ocorrerem contingências de acesso motivadas por fatores técnicos que levem à indisponibilidade de serviço, sendo a conduta da DAB a prevista nos termos das suas condições gerais/especiais de prestação de serviço da DAB às quais esta política de privacidade é complementar, constituindo-se como anexo obrigatório. Na parte de indisponibilidade técnica de acesso ao serviço, poder-se-á dar o bloqueio de acesso para: i) Segurança dos próprios dados contra acessos ilegítimos, por exemplo quando hajam excessivas tentativas de *login* falhadas; ii) Segurança de preservação de dados, quando seja do conhecimento da DAB que os conteúdos correm riscos de ser corrompidos por se manterem disponíveis *online*; iii) Para cumprimento de uma ordem

judicial ou outra com a mesma força compulsória; iv) Nos termos da lei quando a DAB tenha conhecimento de atividade ou informação cuja ilicitude seja manifesta.

3 - Direito à portabilidade

Intrinsecamente ligado ao direito ao acesso, ganha forma diferenciada o direito à portabilidade.

O titular dos dados, além de acesso passa a ter o direito de exigir uma cópia em formato de uso comum, exportável e importável de forma automática/digital, adquirindo, assim, uma autonomia diferenciada já que pode transmitir esses dados a outro(s) Controlador(es)/Responsável(eis) pelo tratamento, ou seja, quebra a indução do atrito à mudança provocada pelo(s) Controlador(es)/Responsável(eis) pelo tratamento.

A DAB, enquanto Controlador/Responsável pelo tratamento, permite ao titular dos dados, através da sua área de cliente, exportar todos os seus dados pessoais num formato universal podendo assim ser importado por qualquer software. Poderá saber mais e como na PARTE II desta PP.

Como Processador/Subcontratante, não conhecendo, por natureza, os dados pessoais que processa, limita-se a veicular o acesso permanente aos seus clientes – Controlador(es)/Responsável(eis) pelo tratamento dos dados - para que estes possam fazer cópias dos conteúdos a qualquer altura, bem como migrar os conteúdos alojados nos seus servidores para qualquer outro provedor de serviços ou, para um dispositivo de armazenamento a ser disponibilizado por este. Também nos serviços conexos ao alojamento de dados e que também possam ter dados pessoais, como nos nomes de domínio, o cliente poderá transferi-los a todo o tempo, no entanto, caso pretenda apenas remover o nome de domínio tal terá que ser requerido ao *registry*. Dado o enorme número de *TLD*s existentes com diferentes regras entre si, e uma vez que a DAB é aqui, também, Subcontratante, deverá o Responsável pelo tratamento (cliente da DAB), caso pretenda, solicitar essa e outras informações sobre o *TLD* pretendido no ato da sua subscrição.

A DAB, apenas terá acesso a estes dados quando seja este o único meio tecnicamente viável, e apenas durante o tempo em que se afigure estritamente necessário, para a prestação do serviço contratado. Nestes casos, a DAB comunicará com o Responsável pelo tratamento (cliente da DAB) os termos técnicos em que tal foi e/ou será feito e

exortará a este para que mantenha os cuidados necessários para garantir a segurança da informação. À indicação destas boas práticas por parte da DAB, é expectável o seu seguimento por parte do Responsável pelo tratamento (cliente da DAB), tal irá prevenir falhas de segurança, bem como exonerar a DAB de qualquer responsabilidade por ação ou omissão advinda do desenvolvimento normal das suas tarefas, uma vez que obriga o Responsável pelo tratamento (cliente da DAB) a auditar e verificar todas os trabalhos levados a cabo, bem como a segurança, conformidade e integridade da informação. Assim ficará o Responsável pelo tratamento (cliente da DAB) obrigado a reportar oportunamente (i.e., imediatamente após a intervenção da DAB) quaisquer anomalias ou desvios que possa ter diagnosticado em resultado desta auditoria obrigatória, para que possam ser prontamente corrigidos e tratados, ou, caso aplicável, devidamente encaminhados para tratamento conforme a política de fuga de informação e de dados pessoais.

Boas Práticas: Normalmente, ser-lhe-ão enviadas no email de intervenções necessárias, as boas práticas a serem usadas para a situação em concreto. Ficando desde já, e pela presente, assegurado e garantido pela DAB enquanto Subcontratante, e aceite pelo Responsável pelo tratamento (cliente da DAB), que o acesso a determinados dados não equivale à sua consulta ou manipulação por parte da equipa da DAB.

O Responsável pelo tratamento (cliente da DAB) entende e aceita que, no âmbito das suas obrigações profissionais a DAB possa ter que aceder aos dados que o Responsável pelo tratamento (cliente da DAB) tem alojados na infraestrutura da DAB, de forma a levar a cabo uma ação que lhe é exigida, e para que tal seja possível poderá ser necessário acesso a dados de *login* a um serviço, e consequentemente o acesso a dados alojados em serviço.

Entendendo ambas as partes que este tipo de informação é sensível e o seu conhecimento deve ser apenas do respetivo titular, a DAB compromete-se a solicitar acesso, apenas quando é estritamente necessário. Nestes casos, ainda que as nossas plataformas sejam seguras, o Responsável pelo tratamento (cliente da DAB) deverá tomar precauções adicionais antes de nos facultar os dados de acesso: i) Alterar a *password* atual para uma aleatória antes de a enviar ao nosso suporte; ii) Depois da ocorrência

estar resolvida, a *password* deve ser alterada novamente; iii) O envio da *password* deverá ser feito em resposta ao *ticket* e através do my DAB - https://my. DAB.pt - que dispõe de acesso seguro; iv) Caso seja solicitado acesso *root* (serviços dedicados) serão disponibilizadas as chaves públicas de acesso que devem ser autorizadas; v) Caso utilize *firewall* agradecemos que nos informe para que possamos enviar lista de endereços IP a autorizar; vi) Imediatamente depois da intervenção da DAB deverá auditar e verificar os trabalhos levados a cabo, bem como a segurança, conformidade e integridade da informação, reportando imediatamente qualquer anomalia ou incongruência de dados; vii) Exortamos que o Responsável pelo tratamento (cliente da DAB) mantenha os softwares alojados e/ou código utilizado devidamente atualizados de forma a não apresentar vulnerabilidades ou falhas de segurança que exponham a informação ao risco, bem como levar a cabo, regularmente, auditorias de segurança aos seus conteúdos; viii) Exortamos que o Responsável pelo tratamento (cliente da DAB) tenha uma política restrita de higiene e segurança de *passwords*, bem como de cópia de segurança dos conteúdos alojados;
iv) Em qualquer caso em oferta de dados pessoais se afigure como inultrapassável para conseguir suporte junto da DAB, deverá ficar advertido que, nestas vias de contacto, existe sempre maior exposição ao risco. O tratamento e processamento destes dados reger-se-á pela parte II da POLÍTICA DE PRIVACIDADE e, neste caso, para exercer o direito de esquecimento de comunicações ou para reportar qualquer situação concernente com risco ou violação de segurança de dados queira fazê-lo por email endereçado a dpo@dab.pt, indicando o nome/código/data/hora/meio/ das comunicações que pretende que sejam esquecidas.

4 - Direito ao esquecimento

O direito ao esquecimento ou "*Right to erasure*" é uma das mudanças fulcrais introduzidas pelo RGPD. Quando antes cabia ao titular dos dados o ónus da prova quanto ao facto dos seus dados, ao estarem a ser processados ou disseminados serem causa direta de danos ou sofrimento para si, agora inverte-se o ónus, passando o direito a ser sempre invocável a todo o tempo.

Portanto, o titular poderá reivindicá-lo sempre, sendo ónus do(s) Controlador(es)/Responsável(eis) pelo tratamento provar(em) razão legalmente fundamentada para não o fazer.

O princípio subjacente a esta mudança no direito é facilitar e agilizar a eliminação, o fim do processamento ou disseminação de dados pessoais de quem assim não pretenda e quando, para tal, não haja uma razão justificada.

Estas razões justificadas que permitem ao(s) Controlador(es)/Responsável(eis) pelo tratamento negar o exercício deste direito ao titular dos dados devem pois, sempre, ser avaliadas à luz de um exercício de razoabilidade que nos obriga a pesar a importância dos interesses legítimos do(s) Controlador(es)/Responsável(eis) pelo tratamento, face aos interesses ou direitos e liberdades fundamentais do titular dos dados.

O titular dos dados terá o direito inegável de ver os seus dados eliminados e interrompido o seu processamento quando:

• O propósito original, ou o fim a que se destinavam os dados pessoais não existir e os dados em si não forem mais necessários para nenhum fim que lhe seja conhecido ou transmitido;

• Quando o indivíduo não consentiu independentemente do fim;

• Quando não haja sustentação legal para tal;

• Se os dados processados são de serviços prestados a uma criança;

• Em qualquer caso em que os dados sejam processados em violação RGPD.

O(s) Controlador(es)/Responsável(eis) pelo tratamento poderá(ão) negar-se à eliminação ou alteração dos dados, provendo, em sua vez, a restrição do seu acesso e/ou processamento quando:

• A precisão dos dados pessoais é contestada pelo titular dos dados, no entanto, a sua exatidão não pode ser determinada ou provada;

• Os dados pessoais que se pretende eliminar ou mudar devem ser mantidos para fins de evidência.

Em qualquer dos casos, o(s) Controlador(es)/Responsável(eis) pelo tratamento é (são) responsável (eis) por comunicar, por escrito, ao titular dos dados, a sua recusa de retificação ou eliminação de dados pessoais ou a restrição do seu tratamento, bem como os motivos da recusa. Sendo ainda facto que a própria lei poderá prever a exclusão a

essa obrigação por parte do controlador(es)/Responsável(eis) pelo tratamento, sempre que esta seja uma medida necessária e proporcional para um estado de direito democrático e, portanto, tendo sempre e devidamente em conta os direitos fundamentais e os interesses legítimos do titular dos dados. São exemplos, não exaustivos, destas exclusões todos os casos em que a eliminação ou alteração de dados possa:

• Evitar prejudicar a prevenção, deteção, investigação ou aplicação de infrações penais ou a execução de sanções penais;

• Pôr em causa a segurança pública;

• Pôr em causa a segurança nacional;

• Pôr em causa os direitos e liberdades dos outros;

• Evitar ou obstruir investigações ou procedimentos oficiais/legais.

Não deixa aqui, no entanto, de ser o(s) Controlador(es)/Responsável(eis) pelo tratamento obrigado a informar o titular dos dados da possibilidade de apresentar uma queixa a uma autoridade de controlo ou de interpor recurso judicial perante a sua recusa a este direito.

Para as entidades Controlador(es)/Responsável(eis) pelo tratamento e processador/Subcontratante a conformidade com o uso deste direito traz várias implicações, começando por aumentar a sua necessidade de capacidade de manter registos de atividades de processamento, bem como provas da relevância e da necessidade de todos os dados que controlam ou processam, o que inclui as finalidades do processamento, categorias envolvidas e prazos previstos. Esta informação deve ser comunicada ao titular dos dados e os registos devem ser mantidos de forma a poderem ser disponibilizados à autoridade de supervisão mediante solicitação de prova para qualquer matéria relacionada a um assunto de dados pessoais.

A DAB, enquanto Controlador(es)/Responsável(eis) pelo tratamento viabiliza ao cliente o direito ao esquecimento quer através da sua área reservada quer por solicitação via email, conforme previsto na PARTE II da PP.

Quanto ao esquecimento dos dados coletados enquanto Controlador(es)/Responsável(eis) pelo tratamento, a DAB, em exercício de razoabilidade, avaliados os parcos dados que coleta face às suas obrigações contratuais e a defesa dos seus interesses legítimos, bem como o cumprimento da lei, nomeadamente a lei fiscal, poderá negar-se à eliminação ou alteração dos dados, provendo, em sua vez, a restrição

do seu acesso e/ou processamento de forma a preservá-lo como evidência. Estes dados são, no entanto, armazenados, não processados, e apenas com acesso restrito e justificado – arquivo morto.

Como Processador/Subcontratante quanto aos dados alojados nos seus servidores pelo Responsável pelo tratamento (cliente da DAB), apesar de agnóstica ao tipo de dados (i.e., se são ou não pessoais) a DAB encontra como intrinsecamente ligado ao tempo obrigatório de retenção de *backups*, caso aplicável, por isso esse será o tempo esse o limite lícito para o direito ao esquecimento neste tipo de serviços. Noutros serviços de alojamento da informação, em que não haja *backups* o direito ao esquecimento será exercido sempre que expressamente requerido ou, automaticamente, após a data de término de serviço, considerando os dias de retenção tendo em vista a recuperação definida para o respetivo serviço, nunca ultrapassando os 30 dias.

O Responsável pelo tratamento (cliente da DAB) entende e aceita, que não é sua responsabilidade direta garantir o exercício de direito ao esquecimento ao titular dos dados quando este seja diferente do próprio Responsável pelo tratamento (cliente da DAB), já que isso envolveria aceder e manipular a dados aos quais não tem legitimidade de acesso. Esta obrigação caberá exclusivamente ao Responsável pelo tratamento (cliente da DAB) que deverá acautelar que esta seja levada a cabo em conformidade com a lei.

Apesar de haver pedido de esquecimento expresso por parte do titular dos dados, ou ainda que esta obrigação resulte do cômputo do tempo, a DAB poderá ser obrigada a preservar dados, quando haja ordem expressa de autoridade judiciária com poderes para o ato ou de forma preventiva para garantir a preservação de provas que possam pôr em causa a segurança pública ou nacional, os direitos e liberdades de outros ou para sua própria proteção e defesa.

5 - Pseudonomização e anonimização

O RGPD recomenda a pseudonimização para reduzir os riscos de exposição dos titulares de dados em causa o que, por si, também viabiliza uma segurança adicional para os responsáveis pelo tratamento e o(s) Processador(es)/Subcontratante(s). Muito embora o

RGPD incentive a utilização da pseudonimização, os dados pseudonimizados não deixam de ser considerados dados pessoais, permanecendo, por isso, abrangidos pelo RGPD.

O RGPD define a pseudonimização, como um processamento de dados pessoais levado a cabo de forma a não poderem ser atribuídos a um sujeito ou dado específico sem o uso de informações adicionais. Para pseudonimizar um conjunto de dados de forma eficiente, as informações adicionais devem ser mantidas separadamente e sujeitas a medidas técnicas e organizacionais que garantam a sua não atribuição a uma pessoa identificada ou identificável.

As técnicas de pseudonimização diferem das técnicas de anonimização. Com a anonimização, os dados são apagados para qualquer informação que possa servir como um identificador de um assunto de dados. A pseudonimização, como vimos, não remove todas as informações de identificação dos dados, mas apenas reduz a vinculação de um conjunto de dados com a identidade original de um indivíduo, usando, por exemplo, a criptografia, que torna os dados originais ininteligíveis e o processo não pode ser revertido sem acesso à chave de descodificação correta ou a tokenização, que é outra abordagem para proteger os dados substituindo-os por outros, chamados tokens.

A distinção legal entre dados anónimos e pseudonimizados é a sua categorização como dados pessoais. Os dados sob pseudónimo ainda permitem alguma forma de reidentificação (mesmo indireta e remota), enquanto os dados anónimos não podem ser reidentificados.

Tanto a pseudonimização como a anonimização são preconizadas pelo RGPD, que aspira e incentiva a sua utilização de forma generalizada e recorrente.

Assim, os Controlador(es)/Responsável(eis) pelo tratamento e o(s) Processador(es)/Subcontratante(es) de dados pessoais são convidados a implementar uma ou outra dessas técnicas para minimizar o risco e, uma vez que as duas técnicas diferem, diante do RGPD, a escolha deverá depender do grau de risco e de como os dados serão processados.

Como Controlador/Responsável pelo tratamento, a DAB usa a pseudonimização, sendo que o uso do ID de cliente, ID de serviço, ID de pagamento ou ID de *ticket* são formas do cliente DAB se, identificar, identificar um serviço, uma determinada transação de pagamento ou interação com o n/ suporte. Internamente, e no tratamento da informação,

tipicamente, o normal operador não precisa conhecer senão o email autorizado do cliente, para sua identificação, já que todas as outras matérias, daí por diante, são tratadas com uso aos referidos ID, Cfr. PARTE II desta PP.

Como Processadores/Subcontratados somos totalmente agnósticos aos dados alojados na nossa infraestrutura, estando limitados a processar os dados, que nos são confiados pelo(s) Controlador(es)/Responsável(eis) pelo tratamento, nos termos necessários para a prossecução das suas obrigações para prestação do serviço contratado. Assim, será responsável por manter a segurança da informação nos termos em que se propõem evitando que os dados sejam acedidos indevidamente quer seja por meios físicos, lógicos ou de engenharia social. Para garantir esta obrigação a DAB tomará todas as medidas de segurança técnicas adequadas à protecção dos dados, onde se inclui a pseudonomização possível dos dados que sejam passíveis de ser acedidos no normal decurso da prestação de serviços, como sendo os nomes dados aos servidores físicos ou dados requeridos por vias de contacto onde não seja viável a confirmação de identidade, por outro lado a total anonimização completa dos dados alojados pelo(s) Controlador(es)/Responsável(eis) uma vez que não são conhecidos da DAB.

6 - Direito à oposição à tomada de decisões automatizadas e à criação de perfil "profiling"

Tomada de decisões automatizadas e *profiling* são dois conceitos distintos, mas muitas vezes interligados.

A criação de um perfil – *profiling* - é uma forma de processamento automatizado de dados pessoais usado para analisar ou prever questões relacionadas a um indivíduo, por exemplo, analisar a sua situação financeira, saúde, interesses ou localização.

A tomada de decisão automatizada é a capacidade de tomar decisões sem envolver a ponderação humana.

Os dois conceitos interligam-se na medida em que o *profiling* pode, na grande maioria das vezes, ser o precursor da tomada de decisões automatizada. Na prática, isto pode processar-se de duas formas, mas antes demais terá sempre de haver uma recolha de dados para traçar um de perfil geral, depois os indivíduos são segmentados em diferentes grupos com base na análise dos dados colhidos.

Partindo daqui, com base neste perfil podem ser tomadas:

• Decisões humanas - onde um humano toma uma decisão baseada no perfil do indivíduo;

• Tomada de decisão exclusivamente automatizada - onde um algoritmo toma uma decisão, sem intervenção humana.

O RGPD vem proibir certos tipos de tomada de decisão automatizada, ou seja, as ações baseadas exclusivamente na tomada de decisões automáticas que produzam efeitos jurídicos ou que, de igual modo, afetem significativamente um indivíduo são proibidas. Considerando-se, assim, que todos os atos que afetam significativamente o indivíduo são atos que colidam com os direitos do indivíduo, afetam o seu estatuto legal ou os seus direitos enquanto parte de um contrato. Na prática, e a título de exemplo, poder ter ou não direito a benefícios para habitação, entrada numa fronteira nacional, recusa automática de um pedido de crédito *online*, recrutamento eletrónico sem qualquer intervenção humana, publicidade segmentada por perfil que leva a diferentes pessoas possam ser cobradas em diferentes preços, etc.

Excetua-se desta proibição os casos em sejam necessárias para o desempenho de uma determinada tarefa, haja consentimento explícito do titular dos dados ou estejam previstas num contrato e ainda quando sejam autorizadas por lei.

No caso, mantendo-se o *profiling* as tomadas de decisão exigirão uma certeza quanto à forma da tomada de decisão e, naturalmente, o impacto e consequências para o indivíduo.

Além desta proibição fica ainda preceituada a obrigação de salvaguardas e transparência. Ou seja, os indivíduos devem ser avisados quando uma decisão foi tomada usando exclusivamente decisões automatizadas, sendo-lhes sempre concedido o direito de solicitar uma revisão dessa decisão. A revisão deve ser realizada necessariamente por humano com autoridade e capacidades apropriadas para alterar a decisão e deverá considerar todos os dados relevantes e toda a informação adicional fornecida pelo indivíduo, além dos dados recolhidos por *profiling*.

Além disto, os titulares dos dados têm sempre o direito a opor-se ao uso de *profiling*, ou a qualquer forma automatizada de processamento de informação pessoal, com o objetivo de os avaliar e tipificar.

Na DAB não há tratamento automatizado, incluindo a definição de perfis que produzam decisões com efeitos jurídicos.

B - Responsabilização

1 - Obrigação do uso da *privacy by design, privacy by default e Data Minimisation*

Privacidade por design – *privacy by design* - como um conceito passa a ser parte de uma exigência legal do RGPD. A privacidade por design exige a inclusão da proteção de dados desde o início do design dos sistemas, portanto deve ser projetada no desenvolvimento dos processos de negócios para qualquer produto ou serviços, sendo definidas configurações de privacidade de elevado padrão e recorrendo a medidas técnicas e de procedimentos capazes de garantir que o processamento, durante todo o ciclo de vida dos dados, estando em conformidade com o regulamento.

É ainda exigido que os responsáveis pelo tratamento mantenham e processem apenas os dados absolutamente necessários para o cumprimento de seus deveres e para cumprimento das finalidades para as quais foram recolhidos e são tratados (minimização de dados), bem como o acesso a dados pessoais seja limitado àqueles que precisam realizar o processamento.

O RGPD vem ainda garantir que são colocados em prática todos os mecanismos e técnicas que possam garantir que, por defeito, apenas será recolhida, utilizada e conservada, a quantidade necessária de dados pessoais tendo em conta a sua finalidade. Esta obrigação deve ser considerada durante toda a vida dos dados e do seu tratamento, bem como no seu prazo legal de conservação, considerando para ambos os casos os requisitos diferenciados necessários à sua acessibilidade. Esta obrigação visa assegurar que os dados pessoais não são disponibilizados massivamente ou a um número indeterminado de pessoas ou sem intervenção humana.

Todas estas medidas trazem a responsabilidade acrescida ao(s) Controlador(es)/Responsável(eis) pelo tratamento/processador/Subcontratante que fica, assim, adstrito, desde a conceção e durante todo o tempo em que processe ou controle dados pessoais, a garantir a privacidade dos titulares dos dados, o que conduzirá, necessariamente, à minimização da exposição ao risco.

Enquanto Controlador(es)/Responsável(eis) pelo tratamento, a DAB cumpre com os requisitos inerentes ao que se entende por *privacy by design* e *by default*, usando os meios de segurança adaptados, com certificados de segurança e pseudonomização desde a subscrição de serviço, encriptação de dados, *firewall*, antivírus & *antimalware*, acessos autenticados por VPN controlados, restritos e escalonados, arquivo reduzido, não guardando *password* e com rigorosa política de limpeza de sistemas internos ciclicamente.

Enquanto Processador/Subcontratante, a DAB garante:

· Os acessos físicos à sua infraestrutura, controlados por Circuito Fechado de Televisão, são controlados 24 horas/dia pelo pessoal responsável da segurança. Existem câmaras nas zonas comuns tanto nos interiores como nos exteriores e o acesso às salas técnicas é totalmente proibido; sistema do controlo global para a deteção de presença de intrusos no edifício. A segurança baseia-se na presença de pessoal 24x7 que dispõe de todos os sistemas necessários para o controlo de todas as zonas do edifício desde o posto de controlo. A segurança é ainda responsável pelo registo humano de acessos aos quais acresce o controle por RFID;

· A nossa rede é composta por trânsito de vários operadores Tier 1, presença em vários pontos de troca de tráfego (GigaPix, ESpanix, DE-CIX), bem como múltiplos acordos de peering privado;

· Os vários *Datacenters* encontram-se interligados permitindo trocas de tráfego público e privado de forma segura e com latências reduzidas. Como opção disponibilizamos serviço de VPN quer seja "*client to site*" ou "*site to site*", permitindo acesso seguro e por rede privada aos serviços e infraestrutura alojada nos vários *Datacenters*;

· Toda a infraestrutura é monitorizada 24x7x365 a partir dos nossos NOC, disponibilizando gráficos com métricas e latência de acesso aos serviços para os vários clientes (serviços que o incluam). Em caso de eventos, a equipa de operações é notificada e são tomadas as ações necessárias à normalização do serviço. Possuímos *SIEM* (*security information and event management*) eficiente bem como política de Gestão de vulnerabilidades, com Monitorização 24x7x365.

2 - Encarregado de Proteção de Dados ("*DPO - Data Protection Officer*") é o responsável pelo tratamento e proteção dos dados pessoais.

A nomeação de *DPO* será mandatória para autoridades públicas, com exceção dos tribunais ou autoridades judiciárias independentes, quando atuem no exercício das suas funções judiciais. Além das autoridades públicas será obrigatório um *DPO* para todos os Controlador(es)/Responsável(eis) pelo tratamento e Processador/Subcontratante, cujas atividades principais consistam em operações de processamento de dados de forma regular e sistemática e em larga escala ou quando esses dados pertençam a categorias especiais – dados sensíveis. Segundo o art.º 9 do RGPD são dados sensíveis todos os que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

O *DPO* deve ser nomeado com base nas suas qualificações profissionais com especial enfoque no conhecimento técnico sobre legislação e práticas de proteção de dados.

O *DPO* é o responsável pela conformidade e pela gestão de processos tendo em vista a segurança de dados. É ainda responsável por lidar com situações de crise, como fugas de informação ou outros problemas críticos para continuidade de negócios no que concerne à manutenção e processamento de dados pessoais e confidenciais.

Mesmo nas entidades em que não seja obrigatório o *DPO*, a entidade deverá designar um responsável pelo tratamento, ou seja, uma entidade, funcionário ou não que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais.

A DAB tem um *DPO* que poderá ser contactado diretamente para o email dpo@dab.pt.

3 - Responsabilidade por fundamento na coleta e processamento de dados

Os dados não podem ser coletados ou processados sem que haja um fundamento legal que o justifique.

Em termos de complexidade, o essencial fundamento será sempre o consentimento expresso por parte do titular, não podendo este ser generalista, mas antes elencar e especificar cada um dos fins a que se destina.

Fora o consentimento, o processamento, por ser indispensável para a prestação de um serviço ou venda de um produto, pode afigurar-se como necessário e a esta necessidade

será intrínseca a necessidade de processar os dados para a preparação e execução de um contrato, acordo, proposta ou outro documento oficial ou com força legal.

O processamento é sempre necessário e justificado para o cumprimento de uma obrigação legal à qual o(s) Controlador(es)/Responsável(eis) pelo tratamento está(ão) sujeito(s) ou para acautelar interesses vitais do titular dos dados ou mesmo de outros que destes dependam.

Tem pleno assento e justificação legal todo o processamento que cumpra obrigações necessárias para levar a cabo uma tarefa de interesse público e para defender os interesses legítimos do(s) Controlador(es) Responsável(eis) pelo tratamento/processador/Subcontratante. Ficando a salvaguardo que a ponderação desses interesses legítimos deve sempre ser sempre feita atendendo aos direitos, liberdades e garantias fundamentais do titular dos dados, já que, em casos em que estes últimos prevaleçam, exige-se sobretudo a proteção dos dados pessoais, em particular se o titular dos dados for uma criança.

Além destes, resulta como intrínseco às suas funções que o processamento dos dados seja levado a cabo legitimamente, no ato do próprio exercício da autoridade oficial do(s) Controlador(es)/Responsável(eis) pelo tratamento (*DPO* ou responsável pelo tratamento e proteção dos dados pessoais), pelo que neste caso o seu acesso e tratamento estará, desde logo, acautelado.

Como Controlador/Responsável de tratamento, a DAB além de minimizar a coleta de dados ao estritamente necessário, tem o seu fundamento legal na subscrição dos serviços por cláusulas contratuais gerais, e ora assim, na necessidade intrínseca à sua prestação. Fora os dados necessários para a subscrição de serviço e para estabelecer contacto com o cliente, a DAB não recolhe ou processa quaisquer outros dados e todos os que lhe possam ser facultados pelo titular de forma voluntária e discricionária são ignorados e excluídos de processamento, tal como previsto na Parte II desta Política de Privacidade.

Como Processador/Subcontratante a DAB garante a todos os seus clientes que leva a cabo as medidas técnicas e organizativas adequadas para cumprimento da lei e de forma a assegurar a segurança da informação e a defesa dos direitos do titular dos dados.

Enquanto Processador/Subcontratante, todos os dados armazenados nos nossos servidores foram recebidos com base na contratação do referido serviço e assim prevalecem enquanto o serviço/contrato prevalecer. Fora este tempo fica a obrigação residual, também advinda do próprio contrato, de manter, durante os tempos definidos os *backups* dos conteúdos anteriormente alojados.

O Responsável pelo tratamento (cliente da DAB) entende e expressamente autoriza de forma geral que a DAB, enquanto sua subcontratante, respeitando as condições que lhe são impostas pela lei, possa subcontratar serviços, que pela sua natureza assim o exigem, como sendo licenciamento; nomes de domínio; certificados *SSL*; sistemas de *backups* e filtragem de email (alojados na infraestrutura da DAB); sistemas de mitigação de ataques etc. Salvaguardando que em todos estes serviços apenas será veiculado acesso a dados pessoais na limitação dos estritamente necessários para:

1 – Registo ou alteração de dados no que concerne a nomes de domínio;

2 – Subscrição e instalação de certificados *S/MIME* (PersonalSign);

O Responsável pelo tratamento (cliente da DAB), ao aceitar esta política de privacidade na subscrição de um dos serviços que assim o exija, estará ainda a autorizar esta subcontratação, sendo que quaisquer informações sobre os subcontratados da DAB serão oferecidas ao Responsável pelo tratamento (cliente da DAB) sempre que solicitadas e quaisquer as alterações a estes subcontratantes ser-lhes-á comunicada viabilizando a sua oposição. Para cumprimento desta obrigação, sempre que pretenda ou tenha necessidade de alterar os subcontratados que possam ter acesso a dados pessoais do Responsável pelo tratamento (cliente da DAB), a DAB comunicará ao Responsável pelo tratamento (cliente da DAB) através de email informativo, tendo o Responsável pelo tratamento (cliente da DAB) cinco dias para se
opor a esta alteração no que aos seus dados pessoais diz respeito.

O Responsável pelo tratamento (cliente da DAB) entende e aceita que para a prestação destes serviços específicos que a DAB é obrigada a subcontratar, poderá ter de enviar, de forma confidencial, os dados pessoais que coleta, para provedores de serviços externos.

O Responsável pelo tratamento (cliente da DAB também entende e aceita que para a prestação do serviço subscrito a DAB terá que enviar os dados necessários para esse fim, aos provedores de serviços externos, subcontratados da DAB, sediados na UE ou fora da

UE, especificamente EUA ou *registrar/y* do país de origem do *ccTLD* subscrito. Considerando que, sem a transferência destes dados, o serviço não pode ser prestado, a aceitação da presente política de privacidade e a subscrição do serviço são prova que o Responsável pelo tratamento (cliente da DAB) aceita os presentes termos.

Pela ação de aceitação das cláusulas contratuais gerais onde se insere a presente Política de Privacidade, aquando da subscrição do serviço, consubstancia-se um vínculo contratual, entre DAB enquanto Processador/Subcontratante e o Responsável pelo tratamento (cliente da DAB), nos termos do artº28/6 e 9 do RGPD. Assim se estabelece, nessa data, como objeto do contrato, a natureza e a finalidade do tratamento dos dados, o serviço contratado, a duração do tratamento, a periodicidade

escolhida, e ficado ainda definido que a DAB desconhece, porque não lhe é necessário ou dado a conhecer o tipo de dados pessoais, bem como as categorias dos titulares dos dados.

Sendo nesta PP dadas a conhecer as obrigações e direitos do Responsável pelo tratamento (cliente da DAB), a DAB obriga-se a:

• Apenas processar os dados para prestação do serviço subscrito, nos termos das suas Condições Gerais/Específicas e presente PP e eliminá-los-á depois de concluída a prestação do serviço, podendo o cliente aceder-lhes antes da data de término para deles fazer cópia ou migração, uma vez que estão sempre ao seu dispor (com exceção das situações acima descritas que lhe sejam exceções);

• Auxiliar, no limite das suas competências, o Responsável pelo tratamento (cliente da DAB), demonstrando o cumprimento das suas obrigações previstas pelo RGPD e prestando as informações e as evidências necessárias para que este último possa responder a inspeções e auditorias. Sendo ainda a sua obrigação comunicar ao Responsável pelo tratamento (cliente da DAB), sempre que para cumprimento desse dever possa eventualmente consubstanciar, em si, a violação de obrigações legais.

• Viabilizará sempre acesso ao Responsável pelo tratamento (cliente da DAB) aos dados que tem alojados na infraestrutura da DAB, de forma a poder cumprir as obrigações a que está adstrito pelo RGPD (salvo exceções devidamente previstas e supra elencadas), bem como quando por este solicitada, a DAB agirá no limite das suas competências, de forma

a auxiliar o Responsável pelo tratamento (cliente da DAB) ao cumprimento das suas obrigações de resposta aos direitos dos titulares dos dados

• Que todos os funcionários e colaboradores da DAB estejam sujeitos à obrigação de sigilo e confidencialidade, bem como tenham recebido e recebam formação e informação sobre confidencialidade e segurança da informação e boas práticas. Estando ainda obrigados a uma política de segurança de informação que os obriga a nomeadamente a:

- Fazer cópias de segurança (*backups*), contra o risco de perda acidental
- Proteger os sistemas contra software malicioso (vírus, malware, phishing, ransomware, adware, etc.);
- Restringir e controlar o acesso físico aos equipamentos de trabalho;
- Guardar as passwords em softwares encriptados;
- Garantir a s composição de passwords de segurança forte;
- Utilizar ligações seguras por *VPN* e não utilizar redes abertas, quando acede remotamente à infraestrutura da DAB;
- Não partilhar e manter protegidas as passwords e os códigos de acesso às instalações e aos sistemas;
- Não partilhar nem conceder acesso a terceiros ao correio eletrónico para fins profissionais;
- Não gravar as passwords de forma automática nos sistemas e nos browsers;
- Não utilizar as mesmas passwords para os sistemas da DAB e para usos pessoais;
- Não escrever passwords ou qualquer dado pessoal em papéis, ou outro suporte de fácil acesso, ou caso o faça garantir que é imediatamente após o seu propósito, devidamente destruído.
- Proteger todos os ficheiros de trabalho que contenham dados pessoais, usando *password* para abertura e edição;
- Não instalar software não autorizado em qualquer computador ou outro dispositivo que utilize no âmbito da atividade profissional;
- Utilizar o email de forma prudente e ponderada.
- Não abrir mensagens de email com origem desconhecida ou com anexos que incluam ficheiros executáveis, salvo se tiverem origem fidedigna e se não indiciarem ser phishing ou malware;

- Verificar sempre os end ereços dos destinatários;
- Não seguir as ligações a links de emails suspeitos;
- Enviar informações críticas ou sensíveis, sempre que possível, em formato encriptado, ou de forma repartida por mais que um meio de contacto;
- Caso se detete um vírus no computador ou comportamento anormal desligar a internet e desligar o cabo de rede se existir, não desligar o computador, contactar alguém da área de informática;
- Não utilizar serviços públicos de email, de transferência de ficheiros e ou serviços cloud para troca de dados da organização, salvo quando autorizado;
- Não utilizar ferramentas ou redes sociais (WhatsApp, ou outras) para comunicar assuntos contendo dados pessoais referentes a matérias profissionais, nem enviar informação da organização por emails que não sejam institucionais;
- Não registar o endereço de email profissional em redes sociais;
- Não criar cópias ou arquivos contendo dados pessoais, a menos que seja prévia e expressamente autorizado;
- Não recolher imagens ou som de pessoas dentro das instalações da empresa, salvo situações previstas em regulamento interno, por decisão do responsável ou previamente autorizadas pelos titulares;
- Não publicar imagens ou som de terceiros em *sites* ou nas redes sociais, sem que tal esteja devida e previamente autorizado pelos respetivos titulares;
- Comunicar superiormente, caso detete que tem acesso a dados pessoais fora da sua função;
- Reportar eventual violação de dados pessoais, efetiva ou potencial ao *DPO*.
- Bloquear o computador sempre que se ausente;
- Não tirar *screenshots* ou fotografias ou a dados pessoais;
- Não guardar dados sensíveis localmente no computador;
- Guardar todas as pastas com dados pessoais em local seguro e de acesso condicionado (armários com portas fechadas à chave);
- Manter o posto de trabalho arrumado e cumprir o princípio de "*clean desk*";
- Não fornecer qualquer informação com dados pessoais pelo telefone, a menos que seja possível certificar a identidade da pessoa que solicita a informação;

- Recolher as impressões para impressora de rede o mais rápido possível;
- Não recolher, tratar e/ou armazenar dados pessoais sem estar para isso autorizado;
- Não recolher, tratar e/ou armazenar dados pessoais sem as devidas medidas de segurança;
- Não divulgar dados pessoais a terceiros, salvo outros colegas da DAB e só dentro do estritamente necessário ao exercício das atividades que lhe estão acometidas;
- Recolher apenas os dados pessoais que sejam estritamente necessários para o exercício da atividade e seguindo os procedimentos instituídos, usando sempre que possível pseudonomização;

4 - Prestar contas da conformidade com o RGPD – *Accountability*

No sentido do RGPD, a prestação de contas é a prova de conformidade de uma entidade com o próprio regulamento. Nessa mesma lógica, a responsabilidade é acompanhada de medidas para mostrar a realidade da proteção de dados. É importante observar esses dois aspetos da responsabilidade: a implementação responsável do RGPD e do "relatório".

O RGPD redefiniu que os dados "pessoais" são os dados usados para identificar uma pessoa: "é considerado identificável uma pessoa que pode ser identificada direta ou indiretamente (...), inclusive por referência a um identificador, por exemplo nome, número de identificação, dados de localização ou identificador *online* , ou a um ou mais elementos específicos da sua identidade física, fisiológica, genética, psicológica, económica, cultural ou social ".

Nesse contexto, o RGPD impõe aos Controlador(es)/Responsável(eis) pelo tratamento adaptar o seu funcionamento de forma a garantir (e poder mostrar - "renderizar contas" se traduzirmos literalmente o termo), que os seus tratamentos de dados pessoais cumprem a lei.

Em termos práticos, esta obrigação de prestação de contas traz consigo a figura do *DPO* e do responsável pelo tratamento e proteção dos dados pessoais, mas acima de tudo força estas entidades a manter um registo documental dos processamentos realizados sob a responsabilidade do(s) Controlador(es)/Responsável(eis) pelo tratamento ou Processador/Subcontratante e a analisar as consequências concretas desse

processamento de dados, apresentando, em conclusão, os riscos particulares no que diz respeito aos direitos e liberdades dos titulares desses dados.

Em suma, pretende o regulamento que o(s) Controlador(es)/Responsável(eis) pelo tratamento de dados deva ser capaz de provar que cumpre todas as obrigações de proteção de dados e que todas as medidas apropriadas foram tomadas para proteger efetivamente os dados coletados.

Enquanto, Controlador/Responsável pelo tratamento de dados e enquanto Processador/Subcontratado, a DAB garante o cumprimento do RGPD e da Lei n.º 67/98 de 26 de Outubro. Para tal, foram tomadas as medidas necessárias ao seu alcance, além das já indicadas, e das que serão ainda indicadas na parte II desta Política de Privacidade, foram criadas ou adequadas as seguintes políticas e processos:

- Política de Privacidade;
- Processo de gestão de incidentes de Segurança de Informação e privacidade que inclui os termos de análise, reação e comunicação;
- BP (*Backup Policy*), política de cópias de segurança para dispositivos internos afetos à prestação de suporte ao cliente e ao serviço; política de cópia de segurança definida por serviço e em conformidade com o contratado.
- Adequação da *AUP (Acceptable Use Policy)*, Política de Utilização Aceitável;
- Política de eventos de fuga de informação que tem como objetivo definir metodologias de ação perante a possibilidade de um evento de fuga de informação de forma a rapidamente a conter, mitigar e resolver.
- Adequação dos Processos de gestão operacional e de gestão de serviço através dos quais se definem procedimentos e instruções de trabalho para orquestrar a gestão técnica da infraestrutura e o suporte ao cliente, desta feita de forma a garantir o fortalecimento das medidas de segurança e o seu cumprimento nos trabalhos habituais;
- Adequação do Regulamento interno para reforçar a adoção de medidas de segurança de informação e de boas práticas junto dos colaboradores.

5 - Fugas de informação e falhas de segurança - *data breaches*

O RGPD define uma violação de dados pessoais como “uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou processados de outra forma”.

Violações de dados pessoais podem ser divididas em três tipos e uma só violação de dados pode envolver, uma, duas ou até as três categorias, a saber:

· Violação de confidencialidade, quando haja divulgação ou acesso não autorizado ou acidental a dados pessoais;

· Violação de disponibilidade, quando houve uma perda de acesso ou destruição de dados pessoais;

· Violação de integridade, quando haja alteração não autorizada ou acidental de dados pessoais.

Com o RGPD o(s) Controlador(es)/Responsável(eis) pelo tratamento, mais do que responsável por evitar que as violações de segurança aconteçam, passa(m) ainda a ter a obrigação legal de verificar a gravidade da violação e notificar a autoridade supervisora sem demora indevida. A menos que a violação de dados não venha de forma nenhuma a constituir uma violação dos dados pessoais e, portanto, não seja suscetível de resultar num risco para os direitos e liberdades dos indivíduos tendo um efeito prejudicial significativo sobre os indivíduos afetados, i.e., que possam resultar em discriminação, danos à reputação, perda financeira, perda de confidencialidade ou outras desvantagens económicas ou sociais significativas. Fora esta exceção o cControlador(es)/Responsável(eis) pelo tratamento tem um prazo máximo de 72 horas após tomar conhecimento da violação de dados para fazer o relatório e comunicar à autoridade supervisora.

Quando esse efeito prejudicial seja provado, cumpre ainda ao(s) Controlador(es)/Responsável(eis) pelo tratamento notificar os sujeitos afetados. A notificação deve ser feita em linguagem clara e simples com uma explicação concreta da ocorrência. Prescinde-se da obrigação de aviso aos titulares de dados se o(s) Controlador(es)/Responsável(eis) pelo tratamento de dados tiver(em) implementado medidas de proteção técnicas e organizacionais apropriadas que tornem os dados pessoais ininteligíveis a qualquer pessoa que não esteja autorizada a aceder-lhes, como

pseudonomização ou anonimização ou caso tome(m) medidas subsequentes que afastem o risco de afetação dos direitos e liberdades dos titulares dos dados.

A DAB enquanto Controlador/Responsável pelo tratamento e enquanto Processador/Subcontratante sempre usou de uma política de transparência para com os seus clientes, portanto a obrigação de comunicação será levada a cabo nos termos anteriormente definidos, desta feita cumprindo o procedimento estipulado. Considerando e analisando, em abstrato, os vários tipos de informação e a sua criticidade, a sua eventual exposição a terceiros não autorizados e consequente potencial impacto no caso de um evento deste tipo, foi elaborada uma Política de eventos de fuga de informação. Esta política estabelece procedimentos específicos, com instruções de trabalho claras para, face a um facto concreto, qualquer sujeito estar apto a analisar e a reagir de forma eficiente e rápida respondendo à necessidade de contenção e solução do problema no menor tempo possível. Tendo em conta as obrigações específicas concernentes a dados pessoais em concreto, para que melhor se adeque a reação a um incidente de privacidade, foi criado um procedimento específico para gestão de incidentes de Segurança de Informação e Privacidade.

Este procedimento é o que garante uma análise equilibrada e devidamente guiada sobre o evento, que no estrito cumprimento do RGPD, permite aferir as necessidades de ações subsequentes, como sendo a obrigatoriedade de comunicação ou não deste evento ao cliente e à CNPD. Todas estas ações ficam devidamente registadas bem como as suas respetivas justificações de forma a servir de evidência e suporte a qualquer ação investigação superveniente.

C - Supervisão

1 - Autoridade de controlo

Autoridade de controlo nacional definida pela Lei Lei n.º 58/2019

Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo nacional para efeitos do RGPD.

A CNPD é definida na lei como uma entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira para controlar e fiscalizar o cumprimento do RGPD e demais

lei, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais tendo em vista a defesa dos direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.

Para tal, todas as entidades sujeitas ao RGPD e a esta lei têm o dever de colaboração de forma a auxiliar em qualquer processo em que seja requerido, salvo as exceções previstas na própria lei.

Assim, define a CNPD que nos termos do n.º 1 do artigo 35.º do RGPD, os tratamentos de dados pessoais suscetíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares têm de ser precedidos de uma AIPD – (Avaliação de Impacto sobre a Proteção de Dados). Considerando definido, a título exemplificativo, três tipos de situações que preenchem os pressupostos desta obrigação do responsável pelo tratamento de dados, art. 35.º/3 do RGPD, a CNPD é a entidade responsável por elencar, nos termos dos pressupostos do n.º 1 do artigo 35º RGPD, outros tratamentos suscetíveis de implicar esse risco, e que, preenchendo os pressupostos do n.º 1 do artigo 35 integram uma lista complementar que agora se apresenta com a obrigação de ser precedido por uma AIPD - Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados. Esta não é uma lista não exaustiva, mas dinâmica, tal como a sociedade da informação sendo dever de todos os responsáveis por tratamento de dados pessoais de tomar conhecimento desta lista, sem prejuízo de sugerir a todos os que demais, apesar de não constarem desta lista de levarem a cabo uma AIPD.

Considerando que (artº35) pretende o RGPD exigir que o controlador de dados crie uma Avaliação de Impacto na Proteção de Dados (AIPD) nos casos em que exista elevado risco de direitos e liberdades de pessoas singulares, dependendo da natureza, âmbito, contexto e finalidade dos dados e do tipo de tratamento que lhe é dado, vem também estabelecer fatores específicos que ajudam à determinação do que poderá ser considerado alto risco. Portanto, para determinar se uma AIPD é necessária, um controlador de dados deve considerar esses fatores, juntamente com os expostos na lista de tratamento de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados.

- O tipo de dados coletados pela DAB enquanto Controlador/Responsável pelo tratamento de dados pessoais não está abrangida pela obrigação de AIPD;
- Enquanto Processador/Subcontratado, não existe nenhum serviço prestado pela DAB, que pela sua natureza, exija necessariamente a criação de uma AIPD pela DAB ou pelo Controlador/Responsável pelo tratamento de dados que o utilize. A análise sobre a necessidade de uma AIPD dependerá dos detalhes e do contexto da forma como o Controlador/Responsável pelo tratamento de dados usa os serviços subscritos.

Assim:

• A DAB não fornece recursos para executar determinados processamentos automatizados de dados, mas como não conhece os dados que aloja nem o que com eles é feito remete a averiguação da necessidade de resposta a esta exigência para o Controlador/Responsável pelo tratamento de dados pessoais;

• Nenhum serviço em concreto comercializado pela DAB está preparado ou tem como objetivo processar categorias especiais de dados pessoais, por isso os serviços da DAB, na sua natureza não potenciam ou aumentam o risco inerente ao processamento de um Controlador/Responsável pelo tratamento de dados pessoais. Naturalmente que nada impede o Controlador/Responsável pelo tratamento de dados pessoais de usar os serviços da DAB para processar categorias especiais de dados (constantes no artº53/3 ou na lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados;

• Sendo certo que os serviços da DAB poderão permitir ao cliente DAB rastrear ou processar quaisquer tipos de dados, incluindo categorias especiais de dados pessoais, ou de monitorização sistemática de zonas acessíveis ao público em grande escala, como Processador/Subcontratado, a DAB não tem controlo sobre o uso dado aos serviços que presta, concluindo-se que cabe ao controlador de dados, por maioria de razão lógica e por impossibilidade de ser de forma diferente, determinar a utilização apropriada dos dados.

Alinhado com estas considerações, o Controlador/Responsável pelo tratamento de dados deverá fazer uma análise do tipo de dados e tratamento que lhes é dado para avaliar sobre a necessidade ou não de uma AIPD.

No caso de se afigurar necessária, deverá o Controlador/Responsável pelo tratamento de dados ter em consideração que para levar a cabo uma DPIA, deverá, em resumo incluir fatores como:

I - os tipos de dados processados;

II - por quanto tempo os dados serão mantidos;

III - Indicar o local onde estão alojados os dados;

IV - Se e para onde poderão ser transferidos;

V - Quem poderá, além do Controlador/Responsável pelo tratamento de dados, ter acesso a esses dados;

VI - Um juízo de ponderação que avalie a necessidade proporcionalmente quanto às operações de processamento e os seus fins;

VII - Avaliação dos riscos aos direitos e às liberdades dos indivíduos;

VIII - Descrição e evidências que as medidas previstas para lidar com os riscos, incluindo garantias, medidas de segurança e mecanismos para garantir a proteção dos dados pessoais foram levadas a cabo.

Neste caso, o cliente da DAB, Controlador/Responsável pelo tratamento, poderá encontrar a informação necessária por parte da DAB enquanto Processador/Subcontratante, nesta política de privacidade, podendo ainda requerer informações complementares para o email dpo@dab.pt

Caso considere que o tratamento dos seus dados pessoais viola a legislação aplicável em matéria de proteção de dados poderá apresentar reclamação à Comissão Nacional de Proteção de Dados - CNPD - www.cnpd.pt.

PARTE II

Enquadramento e obrigações da DAB enquanto Controlador(es)/Responsável(eis) pelo tratamento de dados A DAB está empenhada em proteger a sua privacidade enquanto CONTRATANTE, bem como de todos os utilizadores das suas plataformas digitais e, como tal, recolhe apenas as informações pessoais daqueles que as facultem voluntariamente, e assim também, apenas as utiliza para os fins para os quais foram fornecidas.

Todos os dados coletados serão nesta política elencados de forma transparente e com integral respeito pelos direitos que assistem ao seu titular.

Conceito de Dados Pessoais:

De acordo com o artigo 4º do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, vertido para os normativos portugueses através da Lei n.º 58/2019 de 8 de agosto, dados pessoais são:

"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 (E-mail) ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular."

1 - Recolha e registo e uso de Dados pessoais:

Os dados serão recolhidos e registados em conformidade e para os fins infra descritos e com as licitudes que a seguir se informam:

a) Cookies e rastreamento: As cookies usadas pela DAB podem ser consultadas na política de cookies sendo que em nenhum caso são coletados dados pessoais. Pontualmente, podemos usar Tags de pixel para nos ajudar a medir a eficácia da nossa publicidade e nos permitir fornecer comunicações de marketing mais direcionadas, neste caso, se houverem dados pessoais coletados permanecerão confidenciais, mesmo que a pesquisa seja conduzida por um provedor de serviços terceirizado em nosso nome.

b) Dados para prestação de serviço: Os dados pessoais recolhidos pela DAB são processados automaticamente e destinam-se à gestão da ficha do CONTRATANTE, dos seus serviços e dos seus pedidos de contacto comercial, apoio e suporte. A recolha e o tratamento de dados pessoais têm ainda como finalidade o seu uso para contactos por parte da DAB para efeitos de:

• Garantir o normal funcionamento do serviço contratado, nomeadamente, fornecendo dados para a sua gestão, pagamento e faturação;

• Comunicar intervenções programadas, reportar problemas e/ou outras situações de relevância e/ ou impacto nos seus serviços ou vias de suporte;

• Promover a comunicação exigida contratualmente, usando a via, para tal, estipulada (Condições Gerais de Prestação de Serviço);

• Envio de questionários de qualidade cujo preenchimento o utilizador poderá livremente declinar.

• Criar nichandles para registo de domínios que são entregues à entidade *registrar*/*registry* sem chegarem a ser guardados pela DAB. Mantendo-se apenas a base legal de solicitação de registo – pedido.

c) Dar seguimento à criação de subcontactos de conta de CONTRATANTE:

Serão coletados no mínimo um email de contacto alternativo ao geral, sendo que podem ser adicionados outros dados que o titular da conta opte por oferecer sobre o seu contacto autorizado. Estes subcontactos pressupõem-se ter dado autorização ao titular da conta para este fim, em todo caso se não concordar ou se houver usurpação de identidade por parte do titular da conta, o subcontacto deverá comunicar à DAB o seu desagrado para dpo@dab.pt para que possa ser eliminado o seu contacto.

d) Suporte ao CONTRATANTE: Qualquer dado pessoal que nos seja discricionariamente enviado por email, telefone ou *livechat* será tratado com a segurança viável e adequada ao meio em que nos for transmitido, no entanto, e para garantirmos a privacidade dos dados pessoais exortamos que seja evitado o envio de dados pessoais por estas vias. Caso a oferta de dados pessoais se afigure como inultrapassável deverá ficar advertido que, nestas vias de contacto, existe sempre maior exposição ao risco. O tratamento e o processamento destes dados reger-se-á pela presente POLÍTICA DE PRIVACIDADE e, neste caso, para exercer o direito de esquecimento de comunicações ou para reportar qualquer situação concernente com risco ou violação de segurança de dados, queira fazê-lo por email endereçado a dpo@dab.pt e indicando o nome/código/data/hora/meio/ das comunicações que pretende que sejam esquecidas.

Lembramos ainda que qualquer endereço de email que permita identificar um indivíduo é considerado um dado pessoal, pelo que, se deseja que o seu contacto seja esquecido, por favor certifique-se que nos informa nos termos supra, evitando ainda oferecer mais dados através de assinaturas personalizadas ou outras vias.

e) Ferramentas de comunicação instantânea: A DAB tem ao dispor do seu CONTRATANTE suporte através de ferramentas de comunicação instantânea que,

quando as use, exortamos que seja evitado o envio de dados pessoais, inclusive emails que possam ser considerados como tal. Caso a oferta de dados pessoais se afigure como imprescindível para dar seguimento ao pedido de suporte deverá ficar advertido que, nestas vias de contacto, existe sempre maior exposição ao risco. Os dados coletados por esta via serão usados somente para a prossecução do fim a que se destina, sem prejuízo de indicação do CONTRATANTE em contrário, ou de serem dados coincidentes com outros já coletados com outro fundamento e licitude. O tratamento e processamento destes dados reger-se-á pela presente POLÍTICA DE PRIVACIDADE e, neste caso, para exercer o direito de esquecimento queira fazê-lo por email endereçado dpo@dab.pt e indicando o nome/código/data/hora/meiodas comunicações que pretende que sejam esquecidas.

f) Resposta a contactos comerciais: mediante a autorização e a solicitação do titular dos dados poderá ser elaborada uma proposta comercial, usando os dados oferecidos e coletados para esse fim Nestes casos, a proposta comercial será armazenada em local próprio, protegido com *firewall*, antivírus & *antimalware*, viabilizando acesso seguro por certificado *SSL*, autenticação por *VPN* e outras medidas técnicas adequadas, bem como privilégios de acesso restritos e escalonados. Estes dados serão mantidos durante seis meses, tendo em vista uma possível adjudicação, salvo se o seu titular exercer o direito ao esquecimento.

• Todas as propostas comerciais rejeitadas são esquecidas, bem como todas aquelas cujo CONTRATANTE não apresente resposta após três pedidos de atualização no período máximo de seis meses sem resposta, salvo se o CONTRATANTE expressamente indicar que pretende que aguardemos a sua decisão por mais tempo.

• Todos os dados de propostas comerciais ou tendo em vista transações comerciais adjudicadas serão mantidas nos termos estabelecidos para o tipo ou tipos de serviços a que se referem.

• Todas as propostas comerciais registadas, para além do mero contacto de email, serão revistas no período máximo de sete anos, assim caso já não esteja em curso a prestação de nenhum dos serviços visados serão esquecidas.

g) Averiguação de Legitimidade e Fraude: Para efeitos de verificação de legítima titularidade, alteração de email autorizado, confirmação de dados fiscais ou despiste de

fraude poderá ser solicitado ao CONTRATANTE que forneça elementos complementares sobre a sua identidade, como comprovativos de morada, número de identificação ou outros. Nestes casos, a DAB compromete-se a coletar o mínimo indispensável para:

• Garantir que se trata do titular legítimo dos serviços que se reclama ao abrigo do contrato de prestação de serviços a que este se obrigou aquando da subscrição de serviços;

• Garantir a veracidade fiscal conforme obrigada pela lei fiscal;

• Afastar a possibilidade de subscrição fraudulenta ou que se configura como tendo em vista a prática de ilícito de forma a acautelar os direitos da DAB e de terceiros.

Estes dados serão coletados pelas vias de suporte normal. Findo o processo, atendendo ao legítimo interesse da DAB e à obrigatoriedade de manter meio de prova, serão preservados os dados coletados, sendo devidamente pseudonomizados. Por pseudonomização entende-se que associado ao CONTRATANTE ficará um código alfanumérico indecifrável senão através de acesso a arquivo morto com autorização restrita e apenas se justificado.

h) Formulários de contacto: Todos os formulários de contacto nas páginas *online* da DAB irão coletar os dados de contacto necessários para que lhe possamos dar resposta, bem como todos aqueles que discricionariamente forem juntos no corpo do email/formulário. Este formulário será integrado numa plataforma de *ticketing* protegida com *firewall*, antivírus & *antimalware*, viabilizando acesso seguro por certificado *SSL* e outras medidas técnicas adequadas, bem como privilégios de acesso restritos e escalonados. Esta entrada será pseudonomizada, não podendo, por abstração, ser facilmente encontrada.

Para garantirmos a privacidade dos dados pessoais, exortamos que seja evitado o envio de dados pessoais por estas vias. Caso a oferta de dados pessoais se afigure como inultrapassável, deverá ficar advertido que, nestas vias de contacto, existe sempre maior exposição ao risco. Para solicitar o esquecimento de comunicações, nesta situação, ou para reportar qualquer situação concernente com risco ou violação de segurança de dados, queira fazer o favor de enviar email para dpo@dab.pt e indicar o *Ticket* ID ou data/hora/endereço de email das comunicações que pretende que sejam esquecidas.

Lembramos ainda que qualquer endereço de email que permita identificar um indivíduo é considerado um dado pessoal, pelo que, se deseja que o seu contacto seja esquecido, por favor certifique-se que nos informa nos termos supra, evitando ainda oferecer mais dados através de assinaturas personalizadas ou outras vias.

i) Recrutamento: Se enviar uma candidatura espontânea ou responder a uma oferta de emprego saiba que todos os CV e dados pessoais por esta via coletados serão integrados e armazenados em local próprio protegido com *firewall*, antivírus & *antimalware*, viabilizando acesso seguro por certificado *SSL* outras medidas técnicas adequadas, bem como privilégios de acesso restritos e escalonados. Todas as candidaturas que não apresentem interesse são eliminadas após avaliação. Todos os candidatos que possam potencialmente vir a ser chamados ficam disponíveis durante 12 meses findos os quais, caso não sejam chamados, a sua candidatura será eliminada. Justificam-se os 12 meses para avaliação de percurso do candidato bem como pela possível oportunidade futura de contratação no legítimo interesse da empresa e do candidato. Todas as candidaturas aprovadas darão lugar a contacto registado com o candidato, tendo em vista diligências de recrutamento futuras. Destas, resultará a contratação ou a rejeição justificada, sendo que neste caso, passarão, por ação humana, a esquecidos em arquivo morto, de acesso restrito e apenas justificado, sendo eliminados ao fim de 5 anos. Justifica-se o armazenamento em ambiente segregado e restrito durante 5 anos para efeitos de avaliação processual do recrutamento no interesse da empresa.

j) Redes Sociais; passatempos; ofertas e formações: Todas as interações que sejam feitas pelas seguintes vias:

• Redes sociais da DAB bem como as partilhas em redes sociais de conteúdos divulgados através dos *Site*, blogs e outras plataformas digitais da DAB regem-se pela POLÍTICA DE PRIVACIDADE da empresa que fornece o recurso usado para partilha ou interação, podendo o utilizador obter mais informações por consulta do Anexo I a esta POLÍTICA DE PRIVACIDADE.

• Participação em passatempos: A DAB poderá promover a coleta de dados por intermédio do preenchimento de formulários de contacto *online*, ou em papel, de forma a viabilizar a submissão de participações dos utilizadores em passatempos ou concursos *online* ou offline por esta organizados.

• Subscrição de alertas/notificações: Recolha de dados para viabilizar o envio de alertas e notificações dos serviços aceites a título gratuito ou experimental pelos utilizadores.

• Participação em eventos ou formações: Recolha de dados com o intuito de possibilitar o registo e gestão de participantes em eventos da empresa ou em que a empresa participa. Todos os dados cuja coleta seja da responsabilidade da DAB e apenas por seus meios, sem recurso a redes sociais, serão tratados nos termos da presente POLÍTICA DE PRIVACIDADE no que concerne aos direitos que ao seu titular assiste.

O tratamento dos dados pessoais que nos sejam disponibilizados por via de redes sociais, entidades externas à DAB, deverão ser tidos como tratados em conformidade com as políticas de privacidade das empresas respetivas, considerando o Anexo I a esta política.

k) Interações em Fóruns e blogs: Qualquer informação que possa divulgar em fóruns ou outras áreas públicas do site da DAB ou da Internet, ainda que ligada à DAB, torna-se informação pública.

Por isso, a cautela ao decidir divulgar informações pessoais nessas áreas públicas caberá ao sujeito que o fizer. Nestes casos, para remoção das informações pessoais divulgadas deverá enviar email para dpo@dab.pt indicando artigo / data /hora / meio / email para que possa ser identificado. No entanto,

pode dar-se o caso da DAB não conseguir remover as suas informações pessoais por não ter acesso ao servidor ou serviço (externo à DAB). Nesses casos informaremos prontamente que não estamos aptos a fazê-lo e porquê.

l) Comunicação comercial: O envio de informações de âmbito generalista e publicitário em relação à DAB e aos serviços por ela prestados são alvo de pedido de consentimento segregado e diferenciado, pelo que a coleta dos dados pessoais para fins comerciais e contratuais não legitima ou viabiliza o envio deste tipo de comunicação. Caso o utilizador pretenda receber esta informação deverá, por ação, subscrever ou consentir no seu envio.

m) Endereços de IP: O endereço de IP quando a sua utilização ou identificação isolada não permita que se identifique o seu titular ou o local de onde é levada a cabo determinada ação não poderá ser considerado um dado privado. A forma como é prestado o serviço de IP e coletado, como informação, pela DAB não viabiliza a identificação de um indivíduo, no entanto, perante a possibilidade de risco este é

pseudonomizado, pelo que no âmbito desta POLÍTICA DE PRIVACIDADE furtar-nos-emos de o considerar como dado privado.

2 - Conformidade da Base de Dados:

Os dados fornecidos estão integrados numa base de dados devidamente regularizada junto da Comissão Nacional de Proteção de Dados CNPD, sendo o seu tratamento automatizado, organizado e mantido diretamente pela DAB de acordo com as leis de proteção de dados.

3 - Contratos e Comunicação com Menores:

Estão vedados os acessos a compras a menores de 18 anos. Os menores que pretendam contactar com a DAB, para acederem às plataformas ou disponibilizarem os seus dados pessoais deverão obter autorização dos pais ou tutores.

4- Retificação, portabilidade e eliminação dos dados fornecidos:

• Retificação de dados: Nos termos da legislação aplicável, assiste ao utilizador o direito de acesso e retificação dos seus dados, ora assim a DAB oferece ao CONTRATANTE o acesso permanente aos seus dados, viabilizando, a sua retificação a todo tempo. A acessibilidade do CONTRATANTE aos seus dados é garantida através de uma área reservada, devidamente protegida, primeiro por obrigatoriedade de autenticação e depois por um certificado *SSL*, bem como outras medidas técnicas adequadas, de forma a, assim, garantir que os dados pessoais do CONTRATANTE estão a salvo do acesso indevido por terceiros não autorizados. Esta área reservada está sujeita a rigorosa política de *backups* que poderá consultar, afastando, assim, o risco de perda parcial, integral ou corrupção. Nesta área reservada o CONTRATANTE poderá atualizar os seus dados pessoais à exceção do email geral e do Número fiscal,

o primeiro por se tratar do autenticador único que titula legitimamente o seu utilizador como proprietário dos serviços e o segundo para garantia da veracidade fiscal. Para alterar estes campos deverá enviar email para contabilidade@dab.pt, salvaguardando, à partida, se pretende ou não que este pedido seja encaminhado, depois de tratado, para o esquecimento.

• Tempo de manutenção de dados, Esquecimento e Eliminação: A DAB compromete-se a manter os seus dados devidamente protegidos com *firewall*, antivírus & *antimalware*, viabilizando-lhes acesso seguro por certificado *SSL*, em alguns casos autenticação por *VPN* e outras medidas técnicas adequadas, bem como privilégios de acesso restritos e escalonados. Poderá a todo o tempo na sua área reservada myDAB exercer o direito ao esquecimento de forma automática e direta, sendo que para tal não poderá ter nenhum serviço ativo. Em caso de haver serviços ativos, o esquecimento apenas será levado a cabo quando as obrigações contratuais da DAB para consigo se extinguirem, portanto, a DAB continuará a prestar o serviço até ao seu término. A DAB não tem nenhum relacionamento direto com os indivíduos cujos dados pessoais são fornecidos, processados ou obtidos pelos Revendedores DAB. Os sujeitos que buscam acesso, ou que buscam corrigir, alterar ou excluir dados imprecisos devem direcionar a sua consulta ao responsável pelo tratamento de dados - Revendedor.

• Esquecimento e *Backups*: Após terminada a prestação de serviço o seu pedido de esquecimento será atendido, no entanto, persistirão conteúdos de backup pelo tempo definido na política de *backups*. Estes dados são, por segurança e privacidade, armazenados, não processados, com acesso restrito e justificado e apenas serão utilizados no caso de haver necessidade intransponível de reposição de um backup que inclua os seus dados.

• Esquecimento e eliminação: Em exercício de razoabilidade, avaliados os parcos dados que coletamos face às obrigações contratuais eà defesa dos seus interesses legítimos, bem como o cumprimento da lei, nomeadamente a lei fiscal, a DAB evita a eliminação ou alteração dos dados, provendo, em sua vez, a restrição do seu acesso e/ou processamento de forma a preservá-lo como evidência no seu interesse legítimo. Estes dados são, no entanto, armazenados, não processados, e apenas com acesso restrito e justificado. Assim, sempre que haja legítimo interesse para acautelar os seus direitos ou os de terceiros, a DAB irá levar a cabo a ação de esquecimento antes da eliminação.

Por esquecimento entende-se mover todos os dados para um arquivo morto de acesso reservado, não autorizado senão por justificação fundamentada e a ficar registada. Para cumprimento da lei, nomeadamente da lei fiscal, o esquecimento poderá ir até ao máximo de 12 anos, findos os quais os seus dados serão eliminados. Os seus dados serão

mantidos fora do esquecimento pelo prazo máximo de oito anos após inatividade total, podendo, no entanto, ser movidos a todo o tempo desde que exerça o direito ao esquecimento.

Para todos os dados pessoais advindos de comunicações, deverá o titular dos dados exercer o seu direito ao esquecimento através de email para dpo@dab.pt indicando código ou ID/ data/hora/meio/email para que possam ser identificados e esquecidos.

• Portabilidade - A DAB permite-lhe exportar todos os seus dados pessoais através da sua área de CONTRATANTE myDAB.

5- Segurança e utilização da sua informação

• Segurança no armazenamento e acesso Os dados pessoais que a DAB coleta estão devidamente protegidos com *firewall*, antivírus & *antimalware* viabilizando-lhes acesso seguro por certificado *SSL*, em alguns casos autenticação por *VPN* e outras medidas técnicas adequadas, bem como privilégios de acesso restritos e escalonados, entre outras medidas técnicas adequadas. Adicionalmente, usamos a pseudonimização no contacto com o CONTRATANTE de forma a evitar a exposição ao risco, desta feita para se dirigir ao suporte, deverá indicar o seu ID de CONTRATANTE em vez do nome, ID de serviço em vez do *hostname* ou domínio, ID de pagamento em vez de descritivo ou informação de pagamento ou ID de *ticket* em vez de endereço de email de envio. Para garantir a sua autenticação deverá sempre usar o email geral ou contacto autorizado. Assim, para afastar o risco do uso de um endereço de email que possa constituir dado pessoal exortamos que seja indicado um email geral que não contenha quaisquer dados pessoais como nome ou data de nascimento, ou em alternativa use o suporte *PIN* para se autenticar. Nos casos em que o CONTRATANTE não consiga identificar ou lembrar-se de qual o email geral associado à sua ficha de cliente, para agilizar o suporte, mas sem prejuízo na segurança da informação, a DAB poderá dar-lhe uma pista deste email. Para tal, o operador poderá usar, por escrito, o uso da camuflagem do endereço de email através da substituição de alguns caracteres por símbolos como * ou #. Ao telefone, o operador poderá indicar o domínio associado ao email ou dar uma pista omitindo partes da totalidade do endereço. Ainda privilegiando segurança, mas afastando a entropia no contacto direto, no que concerne à verificação de identidade, para que possamos prover

respostas imediatas, ainda que de impacto nulo, poderá ser-lhe pedido, além do seu ID de cliente, uma identificação de cliente por dois ou três fatores. Neste caso poder-lhe-á ser pedido, que indique qual o email geral da conta, o número de contribuinte associado, alguns dos serviços da sua conta, dados de morada, IDs de serviço, ou outros que possam evidenciar que o sujeito que nos contacta é de facto o CONTRATANTE.

• Segurança no suporte – boas práticas: Em determinadas situações, no âmbito do suporte, para que nos seja possível proceder à análise e resolução de um problema pode ser necessário o *username* e *password* do seu serviço. Entendemos que este tipo de informação é sensível e o seu conhecimento deve ser apenas do respetivo titular. Tendo isto em mente, apenas solicitamos acesso quando é estritamente necessário.

Ainda que as nossas plataformas sejam seguras, o CONTRATANTE deverá tomar algumas precauções adicionais antes de nos facultar os dados:

1. Alterar a *password* atual para uma aleatória antes de a enviar ao nosso suporte;
2. Depois da ocorrência estar resolvida a *password* deve ser alterada novamente;
3. O envio da *password* deverá ser feito em resposta ao *ticket* e através do myDAB - https://my. DAB.
pt que dispõe de acesso seguro;
4. Caso seja solicitado acesso *root* (serviços dedicados) serão disponibilizadas as chaves públicas de acesso que devem ser autorizadas;
5. Caso utilize *firewall* agradecemos que nos informe para que possamos enviar lista de endereços IP a autorizar.

Se não lhe for possível facultar os dados de acesso, deverá abrir um *ticket* no nosso *suporte* por forma a encontrarmos alternativas seguras. Caso a oferta de dados pessoais se afigure como inultrapassável para conseguir suporte, deverá ficar advertido que, nestas vias de contacto, existe sempre maior exposição ao risco. O tratamento e processamento destes dados reger-se-á pela presente POLÍTICA DE PRIVACIDADE e, neste caso, para exercer o direito de esquecimento de comunicações ou para reportar qualquer situação concernente com risco ou violação de segurança de dados queira fazê-lo por email endereçado a dpo@dab.pt e indicando o nome/código/data/hora/meio/ das comunicações que pretende que sejam esquecidas.

• Os subcontactos da conta do CONTRATANTE: Para adicionar subcontactos na sua conta de CONTRATANTE saiba que deverá confirmar que obteve autorização deste contacto para este fim, sabendo que, para validação, este poderá ser solicitado por email para que o confirme e que, por isso, os seus dados de titular de conta também lhe serão revelados.

6 - Envio ou transferência de informação:

• Compromisso: A DAB compromete-se a não vender nem alugar a terceiros quaisquer dados pessoais enviados pelos utilizadores das nossas plataformas digitais, sem prejuízo de o fazer mediante autorização do utilizador ou quando seja legalmente obrigado.

• Obrigações Legais: A DAB poderá aceder, preservar, partilhar informações do CONTRATANTE com empresas, organizações, entidades governamentais ou indivíduos externos à DAB, por estar de boa fé crente que a lei assim o exige. São estes os casos não exaustivos: as autoridades judiciais, centros de arbitragem, as entidades a quem a lei atribua competências ao nível da investigação criminal, ou que tenham por missão a fiscalização e prevenção do cumprimento da legislação no âmbito, designadamente, da proteção dos direitos dos consumidores, propriedade intelectual, comunicações, segurança, saúde pública e práticas comerciais em geral, etc. A DAB poderá ainda aceder, preservar e partilhar informações do CONTRATANTE quando necessário para: estabelecer ou exercer os direitos legais da DAB ou defender-se contra qualquer reclamação legal, incluindo reclamações e ameaças envolvendo a DAB como entidade gestora de um domínio com base no anonimato do seu titular; investigar, prevenir ou tomar medidas em relação a suspeita de fraude ou outras atividades ilegais; prevenir a morte ou sérios danos físicos a qualquer pessoa; ou investigar violações das condições gerais/especiais de serviço da DAB.

• Para prestação de serviços específicos que dependem de terceiros: A DAB poderá ter que enviar de forma confidencial os dados pessoais que coleta para provedores de serviços externos, nomeadamente para viabilizar a prestação de serviços de certificados de segurança e registo e transferência de domínios.

Sendo que estes parceiros estão sediados na UE e, portanto, em conformidade com as leis de privacidade em vigor, ou quando sejam de fora da UE também declarem a sua

conformidade. Nestes casos, a DAB é forçada a requerer e enviar os seus dados para registo de nome de domínio para um provedor de registos de domínios, *Registry* ou *Registrar*, para cumprir os seus requisitos e dar seguimento ao registo, renovação ou transferência de domínio. Em alguns casos, os nomes de domínio, principalmente para pessoas singulares, já podem ser registados de forma confidencial, sendo ainda viável a alteração de público para confidencial ou vice-versa a todo tempo. No entanto, a DAB terá sempre que coletar e enviar os dados de registo para estas entidades. Se pretender ser informado sobre a POLÍTICA DE PRIVACIDADE de uma entidade *Registry*/*Registrar* de um determinado *TLD* queira fazer o favor de nos contactar indicando qual.

• *WHOIS*: Em determinadas jurisdições ou de acordo com as regras da Corporação para Atribuição de Nomes de domínio ou certos registos, as Informações de Registo de Nome de Domínio devem estar disponíveis e acessíveis ao público por meio de uma pesquisa "*WHOIS*". A base de dados *WHOIS* é acessível publicamente e lista as informações de registo de nome de domínio para um nome de domínio específico, o(s) servidor(es) de nomes para os quais o nome de domínio aponta e a data de expiração e de criação do nome de domínio. As informações de registo de nome de domínio fornecidas são alojadas pela DAB e/ou por um provedor de serviços de terceiros e disponibilizadas ao público por meio de pesquisas de *WHOIS*. Em alguns nomes de domínio, o registo pode ser confidencial sendo viável a sua alteração a todo o tempo. Caso os seus dados de *WHOIS* tenham que ficar disponíveis publicamente e sejam usados para contactos por terceiros, saiba que essas comunicações não partem da DAB e a DAB não controla o uso das informações de *WHOIS* por terceiros.

• Gestão negocial, fiscalidade e estatística: Além de partilhar informações com provedores de serviços de forma confidencial, conforme acima descrito, a DAB pode partilhar com terceiros, de forma contratualmente estipulada como confidencial, informações de identificação várias, agregadas em categorias, com dados pessoais isolados e não direcionáveis, obtidas através de pesquisas com clientes e parceiros, considerando: fins estatísticos, análises de campanhas de marketing, resposta a requisitos para a prestação de serviço subcontratado, auditorias financeiras e fiscais, de qualidade, de segurança, etc.

7 - Perfil e decisões automatizadas: Na DAB não há tratamento automatizado, incluindo a definição de perfis que produzam decisões.

8 - Privacidade na conceção e por defeito: A DAB assegura que, tanto quanto é exigível e atendível, foram adotadas e organizadas as medidas técnicas adequadas para proteger os dados pessoais contra a destruição, alteração e/ou difusão acidental ou ilícita. Qualquer violação da privacidade dos dados pessoais será avaliada e reportada em 72h à entidade competente CNPD, bem como ao(s) titular(es) de dados segundo o processo de gestão de incidentes de segurança e privacidade estabelecido. Caso encontre qualquer risco ou incongruência na gestão de dados pessoais da DAB, deverá alertar-nos para dpo@dab.pt, podendo sempre apresentar reclamação à CNPD – Comissão Nacional de Proteção de dados.

Caso encontre qualquer risco ou incongruência na gestão de dados pessoais da DAB, deverá alertar-nos para dpo@dab.pt, podendo sempre apresentar reclamação à CNPD – Comissão Nacional de Proteção de dados.

9 - Pagamentos

A DAB toma todas as precauções necessárias para garantir a proteção da informação recolhida ao CONTRATANTE e garante que todos os dados de pagamento introduzidos são automaticamente codificados através da tecnologia *SSL - Secure Sockets Layer*, tendo em vista garantir a total segurança nos pagamentos efetuados. Para poder comprovar que a informação está a ser transmitida em segurança, note que surgirá a imagem de um aloquete/cadeado fechado junto do *URL* o que é indicativo que a ligação é segura. A DAB não guarda dados de pagamento. Os dados fornecidos pelo CONTRATANTE para efetuar pagamentos, nomeadamente os relativos aos cartões de crédito, nunca são armazenados pela DAB, sendo utilizados apenas no momento do processamento da transação, sendo que esta é levada a cabo a partir de uma página da entidade bancária, segura e com tecnologias adequadas para garantir que não existe qualquer risco. Assim, não só podemos garantir que os dados do CONTRATANTE não ficam expostos a quaisquer tentativas de intrusão como, nomeadamente, pela não

armazenagem de dados de pagamento podemos garantir que, *in extremis*, caso houvesse um acesso ilegítimo este nunca poria em risco o acesso a dados de pagamento.

10 - Entidade Responsável

A entidade responsável pelo tratamento da Base de Dados é a DAB – Digital Absolut Business - Servidor, Virtualização, Cluster, Datacenters e Telecomunicações, LDA, (doravante designada DAB) sediada na Avenida da República, nº 755, sala 23, Vila Nova de Gaia, 4430-201, com o nº de Identificação Fiscal: 505622912, podendo qualquer interessado entrar em contacto com ela através dos seguintes contactos:

Endereços de Email:

Suporte suporte@dab.pt

Informações Gerais info@dab.pt

Departamento Comercial comercial@dab.pt

Departamento Financeiro contabilidade@dab.pt

Para tratamento de dados pessoais: dpo@dab.pt

Telefone: +351 220 110 220

HeadQuarters: Avenida da República, nº 755, sala 23, 4430-201Vila Nova de Gaia

11 - Limites de Aplicabilidade

Esta POLÍTICA DE PRIVACIDADE não se aplica a dados ou informações pessoais que possam ser submetidas ou coletadas por *sites* de terceiros, alojados na infraestrutura da DAB ou a nomes de domínio registados por terceiros junto da DAB, ou registados pela DAB. Não sendo tais conteúdos ou nomes de domínio propriedade legítima da DAB, esta não tem, sobre eles qualquer controlo. No que concerne a esses dados a DAB será apenas SUBCONTRATANTE e responderá apenas enquanto tal e por isso lembra que as políticas de privacidade de tais *sites* de terceiros devem ser avaliadas pelo UTILIZADOR/CONTRATANTE antes deste enviar os seus dados pessoais. Cumpre ainda informar que a nossa responsabilidade, enquanto SUBCONTRATANTES, acaba na segurança da infraestrutura, portanto qualquer incidente de segurança e privacidade que tenha origem de vulnerabilidades de código de CONTRATANTE, plugins, contas de email comprometidas, emails ou outros ficheiros infetados, e qualquer conteúdo do

CONTRATANTE, será da responsabilidade do gestor dos conteúdos que deverá monitorizá-los para agir preventivamente a uma possível vulnerabilidade ou agir por reação ao incidente nos termos preconizados pela legislação aplicável na matéria de privacidade e tratamento de dados pessoais.

12 - Da Lei

A presente POLÍTICA DE PRIVACIDADE respeita o disposto na legislação aplicável na matéria de privacidade e tratamento de dados pessoais. Neste sentido, poderá ser revista a todo o tempo em função de alterações dos normativos legais que a sustentam, assim como das recomendações das entidades, nacionais e internacionais, competentes na matéria.

Quando haja alterações a esta política de privacidade que alterem a sua versão o CONTRATANTE será notificado via email geral. A informação que coletamos e enviamos ajuda-nos a estar aptos a fornecer a melhor experiência de compra e prestação de serviços, por isso incentivamos os nossos utilizadores a participar, oferecendo-nos o seu consentimento.