ÍNDICE

1. Objetivo e âmbito

No âmbito da sua atividade, o **Grupo Turbomar**, (doravante **TURBOMAR**) onde estão reunidas, entre outras, as empresas **Turbomar – Participações SGPS, S.A., e Turbomar Energia – Equipamentos de Produção e Serviços de Assistência Técnica, Lda.,** desenvolve inúmeras operações que envolvem o tratamento de dados pessoais. Tal tratamento deve obrigatoriamente cumprir as disposições legais em vigor, nos quais assenta a presente Política de Proteção de Dados, adiante designada por PPD.

A presente PPD assenta na necessidade de esclarecer e prestar toda a informação necessária inerente à forma como se deve processar o tratamento de dados pessoais, tendo igualmente por objetivo transmitir uma imagem externa de rigor e segurança, sendo assim transversal a toda a TURBOMAR e respetivos colaboradores.

Todos os colaboradores e Direções/Áreas da TURBOMAR que procedam à recolha e tratamento de dados pessoais são individualmente responsáveis pelo cumprimento da presente PPD.

Os responsáveis de cada Direção deverão garantir que todos os processos da sua área respeitam a PPD e providenciar pela formação dos respetivos colaboradores, os quais deverão seguir e cumprir todos os procedimentos aqui descritos como uma obrigação indissociável das suas funções laborais.

2. Conceitos e Princípios

2.1. Principais conceitos

- Dados Pessoais: Dados pessoais são todas as informações de qualquer natureza e recolhidas em qualquer tipo de suporte, relativas a uma pessoa singular, identificada ou identificável. Considera-se identificável o conjunto de informações que podem levar à identificação de uma determinada pessoa, nomeadamente por referência a um identificador (como por exemplo um número de identificação ou um dado de localização).
  Exemplos de dados pessoais:
  - Nome;
  - Morada ou endereço de e-mail;
  - CV;
  - Número de segurança social ou NIF;
  - Matrícula de veículo;
  - Gravações CCTV (câmaras videovigilância);
  - Folhas de Horas/Recibos de Vencimento;
  - Cartões de visita;
- Dados especiais: dados pessoais 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.
- Tratamento de Dados pessoais: uma operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a alteração, a recuperação, a consulta, a utilização, a transmissão, a interconexão, a limitação, o apagamento ou a destruição.

- Responsável pelo tratamento: a entidade (pública ou privada) que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.
  Em regra, em todas as operações promovidas pela TURBOMAR que envolvam o tratamento de dados pessoais, a TURBOMAR age como entidade responsável pelo tratamento;
- Responsável pela proteção dos dados pessoais: colaboradora Ana Bastos informa e aconselha o responsável pelo tratamento de dados, assim como, os colaboradores que tratem desses dados, das obrigações decorrentes da legislação em vigor. Controla as operações de tratamento de dados e respetivas auditorias, realiza avaliações de impacto e formação sobre proteção de dados, coopera com a autoridade de controlo e subcontratantes quando solicitado. Procede à análise associada às operações de tratamento de dados pessoais, considerando o âmbito, o contexto e as finalidades de tratamento. Qualquer contacto no contexto descrito deverá ser realizado por e-mail: rgpd@turbomar.pt ou por telefone: 214168442.
- Responsável pelo tratamento de incidentes: colaboradora Ana Bastos informa e decide juntamente com a gerência da Turbomar da notificação às autoridades de controlo e aos titulares dos dados e subcontratantes. Perante uma ocorrência de violação de dados pessoais, deve tomar as medidas para atenuar e corrigir os seus efeitos. Qualquer incidente deve ser comunicado por escrito para o e-mail: rgpd@turbomar.pt
- Subcontratante: entidade (pública ou privada) que trate os dados pessoais por conta do responsável pelo tratamento destes (vulgo prestadores de serviço do responsável);
- Terceiro: entidade (pública ou privada) que não seja o titular dos dados, o responsável pelo tratamento ou o subcontratante, mas que estão autorizadas a tratar os dados pessoais.
- Área Responsável: corresponde à Área da TURBOMAR responsável por cada operação que envolva o tratamento de dados pessoais, i.e., a área que define as finalidades e os meios de tal tratamento;
- Área Terceira: corresponde à Área da TURBOMAR que, não sendo Área responsável, necessita de aceder a dados pessoais tratados por outras áreas da TURBOMAR.
- Incidente: violação de dados pessoais originada por uma falha de segurança (física ou lógica) que comprometa a confidencialidade, integridade e disponibilidade de dados pessoais (i.e, que possa levar à destruição, perda, alteração, acesso ou divulgação não autorizada de dados pessoais). Consulte a Política de Incidentes constante do **Anexo II** à Presente PPD.
- Procedimento de Avaliação Prévia de Impacto (AIPD): Procedimento prévio a ser efetuado pela TURBOMAR sempre que um tratamento de dados, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. Consulte o procedimento constante do **Anexo III** à Presente PPD.

2.2. Princípios reguladores do tratamento de dados pessoais

Na recolha e tratamento dos dados pessoais que lhes sejam confiados a TURBOMAR e os seus colaboradores deverão pautar a sua conduta pelos princípios que infra se descrevem.

- Princípio da Transparência, Licitude, Lealdade: o objeto do tratamento de dados pessoais deve ser lícito, leal e transparente;
- Princípio da Minimização: o tratamento dos dados pessoais deve ser adequado, pertinente e limitado ao que é necessário para cumprimento da(s) finalidade(s);
- Princípio da Limitação do Tratamento: os dados pessoais devem ser tratados para finalidades determinadas, explicitas e legitimas, sendo que o tratamento deve limitar-se à(s) finalidade(s) para a(s) qual(is) os dados são recolhidos; por outro lado, os dados devem ser conservados até ao termo da finalidade para o qual foram recolhidos ou, se superior, para cumprimento de prazos legais ou durante a pendência de processos judiciais;
- Princípio da Exatidão: só devem ser tratados dados exatos e atualizados;
- Princípio da Proteção de dados por conceção: dever de, quer no momento de definição dos meios de tratamento, como no momento do tratamento, serem aplicadas as medidas técnicas e organizativas adequadas destinadas a garantir o princípio da minimização e a garantir a confidencialidade, integridade e disponibilidade dos dados;
- Princípio da Proteção de dados por defeito: por defeito, só devem ser tratados os dados pessoais que forem necessários para cada finalidade (quanto à quantidade de dados pessoais recolhidos, ao seu prazo de conservação e à sua acessibilidade).

3. Condições de licitude, formas de recolha e tipos de dados e de titulares

3.1. Fundamentos inerentes ao tratamento de dados pela TURBOMAR

Todos os dados recolhidos e tratados pela TURBOMAR têm por fundamento uma das seguintes condições de legitimidade:

- Consentimento: Quando a recolha é precedida do consentimento expresso, específico e informado do respetivo titular, através de suporte escrito ou via web.

  Sempre que a condição de legitimidade consista no consentimento, o mesmo deve referir expressamente a finalidade do tratamento, remetendo ainda para a Política de Privacidade TURBOMAR. Deve ser assegurado que tal consentimento é prestado por escrito, precedido do seguinte parágrafo:

  (Consinto no tratamento dos meus dados pessoais por parte da Turbomar, para a finalidade de ……., nos termos melhor descritos na Política de Privacidade, disponível em turbomar.info).

  Os referidos consentimentos devem ser conservados em formato físico ou digital, pela área responsável.
- Execução de contrato ou diligências pré-contratuais: quando o tratamento é necessário para a execução de um contrato no qual a TURBOMAR e titulares são parte ou para diligências pré-contratuais.

  Esta condição estará preenchida, nomeadamente no caso de contratos de fornecimento e prestação de serviços.

  Os contratos que contêm a cláusula referente ao tratamento de dados, devem ser conservados em formato físico ou digital, nas pastas das Direções/Áreas correspondentes.

- Cumprimento de obrigações legais: quando o tratamento é necessário para o cumprimento de uma obrigação jurídica.
  Esta condição estará preenchida, por exemplo, no decorrer das obrigações de comunicação de certos dados dos colaboradores da TURBOMAR à Autoridade Tributária ou à Segurança Social.
- Interesse legítimo: quando o tratamento se mostra necessário para a prossecução de interesses legítimos da TURBOMAR ou de terceiros, sem prejudicar os direitos e as liberdades dos seus clientes ou colaboradores.
  Esta condição estará preenchida, por exemplo, no que se refere ao controlo de assiduidade dos colaboradores ou no tratamento de dados de videovigilância para garantir a segurança das instalações da TURBOMAR.

3.2. Finalidades para as quais a TURBOMAR trata dados pessoais

Os dados pessoais recolhidos pela TURBOMAR apenas são processados para fins específicos, explícitos e legítimos. Sempre que sejam recolhidos dados pessoais, os mesmos destinam-se exclusivamente às finalidades expressamente identificadas aquando da recolha.
Seguem as principais finalidades que justificam a recolha de dados pessoais pela TURBOMAR:

- Gestão de colaboradores;
- Gestão e execução de contratos de fornecimento e de prestação de serviços;
- Gestão de clientes;
- Videovigilância para Segurança Física das Instalações e Pessoas.

3.3. Formas de recolha

A TURBOMAR apenas recolhe dados que se mostrem adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para os quais são tratados.
A recolha de dados pode ser feita oralmente, por escrito (nomeadamente através de formulários e contratos), bem como através do website TURBOMAR. Sempre que a recolha de dados seja efetuada através de suportes escritos, os mesmos devem conter um conjunto de parágrafos inerentes ao tratamento de dados pessoais.
Todos os suportes de recolha de dados deverão estar centralizados junto da Direção/Área a que respeitam devendo ser utilizado por cada Direção/Área, em face do tipo de tratamento que pretenda efetuar, o clausulado tipo a ser inserido em cada suporte.
Regra geral, a TURBOMAR recolhe diretamente dados pessoais diretamente junto de cada titular, podendo igualmente ser recolhidos dados pessoais através de fontes públicas (como sites de internet e listas públicas oficiais) ou de entidades parceiras (isto no caso da recolha de dados de colaboradores dessas entidades).

3.4. Tipos de titulares de dados

Em face das atribuições da TURBOMAR, na sua maioria, são tratados dados de pessoas coletivas (empresas e associações). Não obstante, para execução das suas atribuições, podem ser recolhidos e tratados dados dos seguintes tipos de pessoas singulares:

- Clientes e respetivos colaboradores;
- Prestadores de serviço e respetivos colaboradores;
- Participantes em eventos promovidos pela TURBOMAR;
- Visitantes das instalações TURBOMAR.

3.5. Categorias de dados pessoais tratados pela TURBOMAR

Para execução das diferentes finalidades descritas em 3.2, a TURBOMAR recolhe os seguintes tipos de dados pessoais:

- dados de identificação (como o nome, naturalidade, cartão do cidadão ou data de nascimento);
- dados de contacto (como o telemóvel, morada ou e-mail);
- dados de habilitação e situação profissional (como nível de escolaridade e CV);
- dados bancários, financeiros e transações (como IBAN ou número de identificação fiscal);
- dados de localização (ao nível da geolocalização);
- imagens recolhidas através de sistemas de videovigilância.

Em regra, a TURBOMAR não deve recolher dados especiais, como dados de saúde ou dados referentes a contraordenações ou ilícitos criminais.

4. Direitos de Titulares

4.1. Deveres de Informação

Por imposição legal, devem ser prestados junto dos titulares um conjunto de deveres de informação inerentes à forma como os dados são tratados pela TURBOMAR. Tais informações deverão ser fornecidas no momento da recolha de dados (sempre que possível) ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo razoável, de forma clara e acessível, em conformidade com o princípio da transparência.

Em face do tipo de tratamentos operados pela TURBOMAR, as seguintes informações devem ser prestadas junto dos titulares:

a) A identidade e os contactos do responsável pelo tratamento (TURBOMAR);
b) Os contactos do responsável pela proteção de dados
c) A(s) finalidade(s) do tratamento a que os dados pessoais se destinam;
d) O fundamento jurídico para o tratamento;
e) Os interesses legítimos do responsável pelo tratamento ou de um terceiro (quando aplicável);
f) Os destinatários ou categorias de destinatários dos dados pessoais a quem os dados podem ser comunicados;
g) Eventuais transferências para países terceiros (se aplicável);
h) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
i) A existência e forma de exercício dos direitos de acesso, de retificação, eliminação, oposição, limitação do tratamento e portabilidade;
j) Se o tratamento dos dados se basear no consentimento, a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
k) O direito de apresentar reclamação a uma autoridade de controlo.

4.2. Forma de prestação dos deveres de informação

A TURBOMAR disponibiliza suportes de recolha que respeitam todas as obrigações referentes à forma como os dados pessoais devem ser recolhidos e as informações a prestar aos titulares dos dados. Tais deveres de informação são prestados através dos diferentes suportes de recolha (formulários, contratos ou outros) ou da Política de Privacidade disponível em *turbomar.info*, sendo este o documento por excelência para onde devem ser encaminhados todos os titulares de dados.
Não obstante, sempre que exista ou se antecipe que vá existir uma operação que implique um tratamento de dados pessoais, todos os colaboradores da TURBOMAR devem garantir que serão cumpridos os deveres de informação supra descritos.

4.3. Exercício de Direitos

Nos termos da legislação em vigor, existe um conjunto de direitos que os titulares, a qualquer momento, poderão exercer junto da TURBOMAR.

- Direito de acesso: direito que permite obter informação relativamente ao tratamento dos seus dados e respetivas características (nomeadamente o tipo de dados, a finalidade do tratamento, a quem podem ser comunicados os seus dados, prazos de conservação e quais os dados que tem de fornecer obrigatória ou facultativamente).
  Este direito pode ser exercido sem quaisquer limitações.
- Direito de retificação: direito que permite solicitar a retificação de dados, exigindo que estes sejam exatos e atuais, como por exemplo, quando os mesmos estão incompletos ou desatualizados.
  Também este direito pode ser exercido sem quaisquer limitações.
- Direito à eliminação dos dados ou "Direito a ser esquecido": direito de solicitar a eliminação dos dados, quando o titular considere que não existem fundamentos válidos para a conservação dos dados e desde que não exista outro fundamento válido que legitime tal tratamento (como a execução de um contrato ou o cumprimento de uma obrigação legal ou regulamentar).
- Direito à Limitação: direito que permite a suspensão do tratamento ou a limitação do tratamento a certas categorias de dados ou finalidades.
  Quando o titular exercer este direito de limitação, os seus dados pessoais não serão eliminados, mas só podem voltar a ser tratados com o consentimento expresso do titular, ou para efeitos de defesa de um direito num processo judicial.
- Direito à Portabilidade: direito através do qual o titular poderá solicitar o envio dos seus dados, em formato digital e de uso corrente, que permita a reutilização de tais dados. Em alternativa, poderá o titular solicitar a transmissão dos seus dados para outra entidade que passe a ser responsável pelo tratamento dos seus dados.
  Este direito apenas pode ser exercido quando a condição de legitimidade do tratamento seja o consentimento do titular ou a execução de um contrato (não se aplica assim ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública), estando também limitado a tratamentos automatizados.
- Direito de Oposição: direito que permite ao titular opor-se a determinadas finalidades. Um dos exemplos deste direito respeita à oposição a finalidades de marketing.
  Esse direito não pode ser exercido quando existam interesses legítimos que prevaleçam sobre os seus interesses (por exemplo, quando o tratamento seja necessário para a execução de um contrato).

- Direito de Retirar o Consentimento: direito que permite ao titular retirar o seu consentimento, mas que apenas pode ser exercido quando o seu consentimento seja a única condição de legitimidade;
- Direito de reclamação junto da Autoridade Nacional de Controlo (CNPD).

5. Fluxos internos de dados

5.1. Identificação de Direção responsável pelo deferimento de fluxos internos

Cada repositório/base de dados tem o respetivo Departamento Responsável, a quem incumbe determinar as finalidades e os meios de tal tratamento. Em caso de dúvida, solicite junto do colaborador responsável pela proteção de dados, o registo de operações de tratamento de dados com vista a ser confirmada a Direção/Área Responsável por cada tratamento, bem como os fluxos internos já analisados e validados.

Novos acessos a dados pessoais que integrem repositórios/bases de dados entre diferentes Direções/Áreas da TURBOMAR, devem respeitar um conjunto de procedimentos e princípios que regulam tais fluxos internos.

5.2. Forma de pedido de acesso/comunicação - procedimento

- O acesso a dados pessoais que integrem repositórios/bases de dados das diferentes Direções/Áreas TURBOMAR deve ser solicitado, por escrito, à Área responsável pelo tratamento no âmbito do qual os dados foram recolhidos, com as seguintes informações obrigatórias:
  - Identificação dos colaboradores da área terceira que necessitem do acesso aos dados (explicar se todos os colaboradores necessitam de ter acesso ou apenas parte deles);
  - Tipo de repositório/ base de dados a cujo acesso é solicitado;
  - Tipo de dados pessoais cujo acesso é pretendido (descrição da categoria dos dados – ex: nome ou e-mail ou dados de vencimento, entre outros);
  - Finalidade do acesso (i.e. explicação do porquê da necessidade de acesso a tais dados);
  - Período de conservação dos dados (explicar o período temporal durante o qual irão ser tratados os dados, com o compromisso de, findo tal período, se proceder à sua devolução ou destruição).
- Após o envio do pedido, deve ser facultada uma resposta por escrito pela área responsável, resposta essa que, sendo afirmativa, deverá conter o porquê da necessidade e adequação de tal acesso, bem como eventuais limitações que devam ser respeitadas pela Área Terceira.
- O registo de todos os pedidos e respetivas respostas ficará registado numa pasta de arquivo físico ou numa pasta comum a toda a Direção/Área a que diz respeito sendo cada pedido de acesso limitado às Direções/Áreas envolvidas e à Direção Geral da TURBOMAR.

5.3. Princípios que devem ser observados aquando da análise de pedidos de fluxos:

Após o pedido de acesso/ comunicação de dados por parte da Direção Terceira, a Direção Responsável deverá analisar tal pedido com base nos seguintes critérios:

- Adequação: deve ser analisada a adequação da finalidade para a qual os dados são solicitados pela Direção Terceira;
- Necessidade: deve ser analisado se, em face da finalidade que dita tal acesso, existe a efetiva necessidade de acesso total ou parcial aos dados pessoais solicitados.
- Proporcionalidade: além da necessidade, impõe-se ainda à Direção Responsável que verifique se o acesso a tais dados é proporcional face a eventuais riscos na esfera dos direitos, liberdade e garantias dos titulares.

5.4. Forma como deve ser dado o acesso e/ou comunicação de dados solicitados

Regra geral, o acesso aos dados deve ser disponibilizado através dos sistemas internos da TURBOMAR, nomeadamente, através de pasta partilhada no SI da TURBOMAR, à qual terão acesso a área responsável e a Área Terceira.

Deve assim ser evitada a comunicação de ficheiros que contenham dados pessoais, por via de e-mail (com vista a serem evitadas brechas de segurança).

6. Conservação de Dados

6.1. Períodos de Conservação

Todos os documentos que contenham dados pessoais devem respeitar o princípio da limitação do tratamento no que respeita ao respetivo período de conservação. Para cumprimento de tal princípio, devem ser atendidas as seguintes regras: os dados devem ser conservados até ao termo da finalidade para os quais forem recolhidos ou, se superior, até ao termo dos prazos legalmente impostos para conservação de tais dados (ou ainda, casuisticamente, até ao termo de processos judiciais que justifiquem a conservação dos mesmos).

Em face de tais regras, bem como do tipo de operações que envolvem o tratamento de dados pessoais, a TURBOMAR definiu os seguintes prazos de conservação a serem seguidos por todos as Direções/Áreas da TURBOMAR:

- Documentação comercial financeira/fiscal:
  Deve ser conservada pelo período de 10 anos após o termo da relação comercial. A este respeito, quando se tratem dados pessoais de contactos de empresa que não forem necessários para justificar registos de contabilidade, não existirá legitimidade para os conservar após a cessação do contrato, devendo assim ser eliminados após o termo da relação contratual.
- Documentação Laboral:
  Em face dos prazos de caducidade e dos diferentes normativos legais existentes, deverão ser atendidos os seguintes prazos de conservação no que respeita a documentação de colaboradores da TURBOMAR:
  - Dados biométricos: devem ser conservados apenas durante o período necessário para a prossecução das finalidades do tratamento a que se destinam (controlo de assiduidade) devendo ser destruídos após o termo da relação laboral ou caso o trabalhador seja transferido para outro local de trabalho (art.º 18/3 do Código do Trabalho);

- Documentação contratual e inerente a segurança social (ex. contrato de trabalho, documentos relacionados com a cessação de contratos de trabalho, mapas de férias, mapas de horários de trabalho, registos individualizados de trabalhadores, registo de sanções disciplinares, plano de formação profissional e comprovativos das ações de formação profissional, consulta anual aos trabalhadores sobre matérias de segurança, higiene e saúde no local de trabalho, comunicações de admissão e de cessação de contratos de trabalho) deve ser conservada até 5 anos após a cessação do contrato de trabalho (por conta do prazo de prescrição de contraordenações laborais e de Segurança Social);
- Documentação necessária a efeitos fiscais (ex. recibos, retenções na fonte, relatórios AT) deve ser observada durante o prazo de 10 anos após a cessação do contrato de trabalho;
- Documentação relativa a segurança e saúde no trabalho: A TURBOMAR deve manter à disposição das entidades fiscalizadoras competentes, pelo prazo de 5 anos após o termo da relação laboral, os registos relativos à realização das atividade inerentes à segurança e saúde no trabalho (ex. resultados de avaliações de riscos profissionais, lista das situações de baixa por doença e do número de dias de ausência ao trabalho, a ser remetida pelo serviço de pessoal e, no caso de doenças profissionais, a relação das doenças participadas, lista das medidas, propostas ou recomendações formuladas pelo serviço de segurança e de saúde no trabalho, em conformidade com o art.º73-B/5 do Regime Jurídico da Promoção da Segurança e Saúde no Trabalho).
- Processos de recrutamento (cv, avaliações de candidatura e entrevistas) para cargos internos: 5 anos após o termo do processo de recrutamento, nos termos do art.32º do Código do Trabalho;
- Restantes dados pessoais de colaboradores TURBOMAR, não incluídos nas anteriores categorias (como será o caso de dados de familiares, carta de condução ou outros): devem ser anonimizados ou eliminados no prazo máximo de 1 ano após o termo da relação contratual.

- <u>Videovigilância:</u>
  As imagens recolhidas através de sistema de videovigilância devem ser conservadas pelo prazo máximo de 30 dias, findo o qual serão destruídas, só podendo ser utilizadas nos termos da legislação penal e processual penal.
- <u>Dados inerentes a finalidades genéricas da TURBOMAR:</u>
  Dados poderão ser conservados enquanto perdurar a finalidade para a qual são recolhidos, no pressuposto de poder ser sempre garantido o direito de apagamento ou de ser retirado o respetivo consentimento.

6.2. Forma de Conservação

Por forma a serem garantidos os prazos de conservação supra descritos, mostra-se igualmente fundamental regular e restringir a forma como os dados inerentes aos vários repositórios são conservados.

Como tal, deverá ficar estabelecido quem dentro de cada Direção/Área responsável está encarregue da eliminação dos dados uma vez que estes deixem de ser necessários. A eliminação deverá ser feita de modo a garantir que os dados são eliminados no ERP Primavera, como em todos os ficheiros autónomos que contenham os dados do titular, sejam eles físicos ou digitais. Os ficheiros físicos deverão ser destruídos com recurso a uma destruidora de papel ou manualmente até que sejam ilegíveis. Os ficheiros digitais deverão ser eliminados através de software que garanta a respetiva eliminação, incluindo da página de reciclagem.

A pessoa encarregue da eliminação dos dados dentro de cada Direção/Área responsável deverá igualmente certificar-se que os subcontratantes a que recorre também procedem à eliminação dos dados desnecessários.

7. Entidades Relacionadas

7.1. Principais conceitos e princípios

As entidades relacionadas com a TURBOMAR, enquanto responsável pelo tratamento dos dados pessoais, podem ser de dois tipos:

- Subcontratante: entidade (pública ou privada) que trate os dados pessoais por conta do responsável pelo tratamento destes (vulgo prestadores de serviço do responsável);
- Terceiro: entidade (pública ou privada) que não seja o titular dos dados, o responsável pelo tratamento ou o subcontratante, mas que estão autorizadas a tratar os dados pessoais.

Podemos dizer, então, que a diferença fulcral entre os dois tipos de entidades reside no facto de o subcontratante tratar os dados pessoais em nome e por conta da TURBOMAR (enquanto responsável pelo tratamento) e de acordo com as instruções desta última. Exemplos de subcontratantes: empresa que preste serviços informáticos, empresa de segurança que preste serviços de videovigilância nas instalações da TURBOMAR.

Já um terceiro, não obstante ter acesso a dados pessoais da TURBOMAR, não procede ao tratamento de tais dados para concretização de finalidades definidas pela TURBOMAR, mas sim decorrentes do exercício da sua própria atividade. Exemplos de terceiros: uma companhia aérea através da qual a TURBOMAR reserve viagens de avião para os seus colaboradores e ou convidados, uma companhia de seguros a quem a TURBOMAR comunica dados dos colaboradores para efeitos de inclusão ou exclusão do seguro, a Autoridade Tributária ou a Segurança Social, a quem a TURBOMAR, por imposição legal, transmite mensalmente dados dos respetivos colaboradores.

No que se reporta aos subcontratantes, é, ainda, de salientar que impende sobre o responsável pelo tratamento o dever de recorrer apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas para que o tratamento satisfaça os requisitos de segurança, integridade e confidencialidade dos dados impostos pelo RGDP, e assegure a defesa dos direitos do titular dos dados.

Esta especificidade obriga a que a relação com os subcontratantes deva ser regulada por contrato escrito (Acordo de Subcontratação) que preveja a forma como o tratamento dos dados é realizado e quais as medidas que o subcontratante adota no sentido de garantir a segurança e confidencialidade dos dados tratados.

Ainda acerca dos subcontratantes, os mesmos não poderão contratar outro subcontratante (subcontratante ulterior) sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral nesse sentido. No caso da TURBOMAR, será conferida uma autorização genérica para a contratação de subcontratantes ulteriores, incumbindo, no entanto, sobre o subcontratante o dever de informar a TURBOMAR, por escrito, a identificação de tais prestadores ulteriores (dando-lhe assim a oportunidade de se opor a uma eventual contratação).

7.2. Identificação de categorias de Entidades Relacionadas a quem são comunicados dados pessoais

Por referência à distinção estabelecida no ponto anterior, segue uma lista (não exaustiva) dos tipos de entidades relacionadas a quem a TURBOMAR comunica dados pessoais, e a respetiva finalidade da comunicação:

- Entidades subcontratantes:
  - Empresas de segurança (fornecimento de equipamento, serviço de instalação e recolha de Imagens);
  - Prestadores de IT (para suporte informático e técnico);
  - Prestadores de serviços de limpeza;
  - Agência de Viagens (para gestão e marcação de viagens e alojamentos);
  - Advogados (patrocínio de ações judiciais).
- Entidades terceiras
  - Entidades formadoras (para efeitos de formação e emissão de certificados formativos);
  - Companhias áreas e hotéis (para aquisição direta de bilhetes de avião e alojamento);
  - Consulados (para obtenção de vistos);
  - Segurança Social e IGFSS (cumprimento de obrigações legais);
  - AT (para cumprimento de obrigações legais);
  - INE (para cumprimento de obrigações legais);
  - ACT (cumprimento de obrigações legais);
  - Instituições bancária Millenium BCP (para emissão do cartão Sodexo)
  - Seguradora Allianz (para diligências pré-contratuais a pedido do titular dos dados que quer usufruir do seguro);
  - Vaulabor (para cumprimento de obrigações legais).

7.3. Comunicação de Dados a Entidades Subcontratantes

Os contratos com prestadores externos que possam, através de qualquer forma ou suporte, aceder a dados pessoais da TURBOMAR, devem conter obrigatoriamente como anexo um Acordo de Subcontratação, cujo template se encontra disponível junto do responsável pela proteção de dados.

Incumbirá a cada Direção que pretenda contratar prestadores de serviços /fornecedores, informar o referido responsável para completar a minuta do Acordo de Subcontratração, preenchendo, nomeadamente:

- Dados do subcontratante;
- Descrição da prestação de serviços;

- Detalhes do tratamento (Anexo I), com os seguintes itens: Objeto do Tratamento (especificação dos serviços prestados), Natureza e finalidade do Tratamento (especificação das finalidades), Categorias de Titulares dos Dados, Tipo de Dados Pessoais (dados de identificação, dados de contacto, situação financeira, habilitações, entre outros);
- Medidas Técnicas e Organizacionais (Anexo II): anexo a ser preenchido pelo subcontratante e que identifica, nomeadamente, as medidas de controlo de acesso, de disposição, de transmissão e de eliminação.

Incumbirá ao responsável acima referido, diligenciar pelo correto preenchimento e assinatura dos Acordos de Subcontratação, devendo os mesmos ser arquivados em dossier guardado na Direção Financeira.

7.4. Forma de comunicação às diferentes Entidades Relacionadas

A forma de comunicação de dados pessoais a entidades relacionadas assume especial relevância uma vez que o envio de informação/dados através de meios que não garantam segurança, ou o envio de informação/dados a destinatários errados, pode pôr em causa a segurança e a confidencialidade dos dados pessoais e gerar um incidente de violação de dados pessoais (melhor descrito no capítulo "*Violação de Dados*").

Cabe, portanto, a cada colaborador ter a máxima atenção no momento em que comunica dados pessoais a entidades externas, privilegiando sempre a forma de comunicação que garanta a maior segurança dos dados possível.

No sentido de mitigar riscos de segurança na comunicação de dados com as entidades relacionadas, a TURBOMAR tem implementadas as seguintes soluções:

- Regra geral, os dados devem ser enviados através de Portais das entidades relacionadas (como é o caso do Portal da Autoridade Tributária ou da Segurança Social);
- Não sendo possível comunicar dados via Portais, os dados devem ser enviados em formato de ficheiros, em e-mail zipado, com password;
- Outras regras a serem seguidas pelos colaboradores TURBOMAR:
  - Proibição de transferência de dados através de soluções web (wetransfer, wesendit, etc.);
  - Criação de grupos de destinatários previamente definidos como seguros para envio de ficheiros regulares.

7.5. Comunicação de dados para países terceiros

A comunicação de dados a entidades localizadas em países terceiros (fora da EEE – Espaço Económico Europeu) carece de um procedimento mais apertado, incumbindo à TURBOMAR apenas transferir dados para países terceiros ou organizações internacionais que apresentem garantias adequadas nos termos do RGPD.

Daí que, incumba a cada Direção/Área responsável, analisar futuras necessidades de transferência de dados para países terceiros. Em caso de dúvida, deverá ser consultado o responsável pela proteção de dados.

Regra geral, só possam ser efetuadas transferências de dados para países terceiros se:

- Existir relativamente a esse país uma decisão de adequação por parte da Comissão Europeia;
- Existirem regras vinculativas aplicáveis às empresas de um mesmo Grupo;
- Existir entre as entidades um contrato com cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia.

Não sendo possível cumprir uma das referidas condições (como sucederá na maioria das situações), apenas poderão ser transferidos dados para entidades relacionadas, caso:

- O titular dos dados tiver dado o seu consentimento expresso a tal transferência, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;
- A transferência for necessária para a execução de um contrato entre o titular dos dados e a TURBOMAR;
- A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados.

A Administração,

Carnaxide, 25 de maio de 2018

Versão: PPD-RGPD 2018-01

Anexo I – Política de Violação de Dados

I. Conceito e tipificação de *Violação de Dados*

Uma violação de dados pessoais é originada por uma falha de segurança que pode levar à destruição, perda, alteração, divulgação não autorizada de dados pessoais transmitidos, armazenados ou de qualquer modo processados por qualquer entidade.
Uma violação de dados pessoais pode ser intencional ou acidental e pode não se cingir à perda de dados pessoais, abrangendo assim qualquer falha de segurança que comprometa a confidencialidade, integridade e disponibilidade de dados pessoais.
Destacamos os seguintes exemplos de *violação de dados* que podem ocorrer no contexto da atividade da TURBOMAR:

- Acesso por um terceiro não autorizado a sistemas de informação da TURBOMAR;
- Transmissão de dados pessoais para um destinatário incorreto, por exemplo através de envio de e-mail com ficheiro de dados pessoais, para destinatário incorreto;
- Roubo ou perda de equipamento (como um laptop, smartphone ou tablet) que contenha dados pessoais;
- Incorreta gestão de níveis de acesso por parte de utilizadores, nomeadamente através do acesso não autorizado por colaboradores TURBOMAR, a suportes que contenham dados (ex: armários não trancados);
- Eliminação indevida de dados pessoais (em desrespeito por períodos de conservação estipulados pela TURBOMAR);
- Retificação de dados pessoais sem o consentimento expresso do respetivo titular (i.e., sem serem respeitadas as medidas de verificação e segurança implementadas pela TURBOMAR);
- Acesso indevido e/ou perda de backups.

Uma violação de dados pode potencialmente ter uma série de efeitos adversos significativos sobre os titulares dos dados, que podem resultar em danos materiais ou não materiais. Tais danos podem incluir a perda de controlo sobre os dados pessoais, a limitação dos seus direitos, discriminação, roubo ou fraude de identidade, perda financeira, reversão não autorizada de pseudonimização, dano à reputação e perda de confidencialidade de dados pessoais protegidos. Pode também incluir qualquer outra desvantagem económica ou social significativa para os titulares dos dados.
É, portanto, essencial serem adotadas, não só medidas preventivas destinadas a evitar situações de violação de dados pessoais, como também medidas corretivas que garantam uma imediata correção e minimização dos efeitos dos *incidentes*.

II. Notificações de relato de *violação de dados* à Autoridade de Controlo e aos titulares dos dados: em que situações deve ocorrer, forma e prazos

Notificação à Autoridade de Controlo

Uma das principais novidades do novo RGPD respeita ao dever de notificação de violações de dados pessoais junto da Autoridade de Controlo (CNPD).

A CNPD só terá que ser notificada de uma violação de dados pessoais se essa falha apresentar riscos para os direitos e liberdades dos titulares dos dados. Se existir a probabilidade de colocar em risco os direitos e liberdades dos titulares dos dados, a CNPD deverá ser notificada, de contrário, não é necessário que esta seja notificada. Contudo, caso a TURBOMAR decida não notificar a Autoridade de Controlo, deverá ser capaz de justificar tal decisão, sendo, para tal, aconselhável que a falha de segurança e correspondente violação de dados pessoas esteja documentada.

De modo a avaliar o risco para os direitos e liberdades dos titulares dos dados, devem ser equacionadas as potenciais consequências negativas desta violação para os mesmos.

Tratando-se de uma violação que requeira notificação à CNPD, o responsável pelo tratamento deverá notificá-la sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma. Se a notificação for transmitida após o prazo de 72 horas, deverá ser desde logo acompanhada dos motivos do atraso.

Nos termos do n.º 2 do artigo 33.º RGPD, a notificação a enviar à Autoridade de Controlo deverá reunir, pelo menos, os seguintes elementos:

- Descrição da natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
- Descrição das consequências prováveis da violação de dados pessoais;
- Descrição das medidas adotadas ou propostas pela TURBOMAR para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos".

Notificação aos titulares dos dados

Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, nos termos já descritos, o responsável pelo tratamento comunicará a violação de dados pessoais aos titulares dos mesmos sem demora injustificada.

Nos termos do n.º 2 do artigo 34.º RGPD, a notificação enviada aos titulares dos dados deverá descrever em linguagem clara e simples a natureza da violação dos dados pessoais e fornecer, pelo menos, as seguintes informações previstas no artigo 33.º, n.º 3, alíneas b), c) e d):

- Descrição das consequências prováveis da violação de dados pessoais;
- Descrição das medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

Notificação por Subcontratantes

No caso de se tratar de uma *violação de dados* sofrida por um subcontratante, a partir do momento em que este tenha conhecimento da mesma, deverá informar de imediato o responsável pelo tratamento dos dados. Para os subcontratantes não existem exceções ao dever de *relato* de *violação de dados* ao responsável pelo tratamento, pelo que deverão sempre reportar-lhe os incidentes de violação de dados.

III. Como deve o colaborador proceder em caso de suspeita ou *violação de dados*

Sempre que o colaborador tomar conhecimento, ou suspeitar, de um incidente que envolva dados pessoais tratados pela TURBOMAR, ou do qual possa resultar, na destruição acidental ou não autorizada de dados, na perda, alteração, acesso ou revelação não autorizada dos dados tratados da responsabilidade da TURBOMAR, deverá seguir o seguinte procedimento:

1. Relato do incidente, no prazo máximo de 24 horas, junto do responsável pelo tratamento de incidentes, através do formulário que se junta no Anexo A, a ser remetido através de e-mail.
2. O alerta deverá conter uma descrição da violação detetada e de quaisquer medidas corretivas que tenham sido já adotadas (se existentes).
3. Guardar, quando possível, toda a documentação de suporte ou outra evidência da violação detetada e troca de comunicações sobre o tema (registos informáticos que possam ser guardados, troca de emails, *print screens*, entre outros).

IV. Como deve atuar a Área Responsável em caso de *suspeita ou violação de dados?*

Sempre que seja comunicado à Área Responsável Incidentes a suspeita, ou incidente, de violações de dados pessoais, deve ser seguido o seguinte procedimento:

1. O responsável acima referido deve, de imediato, analisar e certificar-se de que a suspeita de incidente, ou o incidente, consubstancia numa violação de dados pessoais, resultando ou podendo resultar, na destruição acidental ou não autorizada de dados, na perda, alteração, acesso ou revelação não autorizada dos dados.
   Caso se conclua que a suspeita ou incidente reportado não consubstancia uma violação de dados pessoais ficam dispensados os próximos pontos.
2. Caso se conclua que a suspeita, ou incidente reportado, consubstancia uma violação de dados pessoais, a colaboradora Ana Bastos deve de imediato, tomar as necessárias medidas corretivas, com vista a estancar as consequências do incidente.
3. Em simultâneo, e até ao máximo de 48h após o alerta da suspeita ou incidente de violação de dados, a referida colaboradora deverá analisar as consequências da violação de dados ocorrida, por forma a concluir se da mesma resultaram ou não riscos que afetem os direitos e liberdades dos titulares dos dados.
   Caso se conclua que o incidente de violação de dados não afeta os direitos e liberdades dos titulares dos dados, a TURBOMAR estará dispensada de notificar a CNPD acerca de tal incidente, competindo-lhe apenas registar a violação de dados pessoais ocorrida, os factos relacionados com as mesmas, os respetivos efeitos e as eventuais medidas de reparação adotadas.

4. Caso se conclua que o incidente de violação de dados afeta os direitos e liberdades dos titulares dos dados, deverá, até ao prazo máximo de 72 horas após o incidente de violação de dados, ser relatado tal incidente junto da CNPD, através de formulário online disponível em www.cnpd.pt.
   A notificação deve conter as seguintes informações:
   - A natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
   - O nome e os contactos do responsável pela proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
   - As Consequências prováveis da violação de dados pessoais;
   - As medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.
5. Caso se conclua que o incidente de violação de dados representa um elevado risco para os direitos e liberdades dos titulares dos dados, a responsável pelo tratamento de incidentes deverá ainda, no mesmo prazo, diligenciar por notificação de tal incidente junto dos titulares dos dados afetados, devendo fornecer-lhes pelo menos as seguintes informações:
   - O nome e os contactos do responsável pela proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
   - As consequências prováveis da violação de dados pessoais;
   - As medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

Anexo A - Formulário de relato de uma violação de dados

1. Identificação do Colaborador

Nome	
Número de Contribuinte (NIF)	
Contato	
Função	

2. Informação do Incidente:

Hora/data início da violação:	
Hora/data fim da violação:	
Hora/data conhecimento da violação:	
Forma como teve conhecimento da violação:	

Tipo de violação:

- ☐ Integridade (alteração indevida)
- ☐ Confidencialidade (acesso ou divulgação indevida)
- ☐ Disponibilidade (eliminação indevida)

Natureza de violação:

- ☐ Equipamento perdido ou roubado
- ☐ Documentos perdidos ou roubados
- ☐ Correio perdido ou acedido indevidamente
- ☐ Hacking
- ☐ Malware
- ☐ Phishing
- ☐ Outra

Causa de violação:

- ☐ Ato interno não malicioso
- ☐ Ato interno malicioso
- ☐ Ato externo não malicioso
- ☐ Ato externo malicioso
- ☐ Outra

Descrição do Incidente:

_____

_____

_____

3. Consequências da violação:

Integridade

A alteração/corrupção dos dados pode ter consequências para os titulares?	☐ Sim	☐ Não
Indique quais:		
A alteração/corrupção dos dados é passível de ser revertida para o estado original?	☐ Sim	☐ Não
Os dados foram cifrados?	☐ Sim	☐ Não

Confidencialidade

A alteração/corrupção dos dados pode ter consequências para os titulares?	☐ Sim	☐ Não
Indique quais:		

Disponibilidade

A perda de disponibilidade dos dados pode ter resultado em consequências para o titular dos dados (durante a violação ou no futuro)?	☐ Sim	☐ Não
Indique quais:		

Notas adicionais:

_____

_____

_____

4. Dados Pessoais:

Tipo de dados pessoais:

- ☐ Dados de identificação (Nome, CC, NIF)
- ☐ Dados de contacto (telefone, e-mail, morada)
- ☐ Dados financeiros
- ☐ Dados sensíveis (ex: dados de saúde)

Outros dados: _____

É possível determinar número sujeitos envolvidos: ☐ Sim ☐ Não

Número de sujeitos envolvidos: _____

5. Titulares de Dados:

Tipo de dados pessoais:

- ☐ Trabalhadores
- ☐ Utilizadores
- ☐ Subscritores
- ☐ Alunos
- ☐ Clientes
- ☐ Menores
- ☐ Outros

Notas Adicionais:

_____

6. Informação aos titulares: (a ser preenchido pelo Departamento Responsável Incidentes)

Titulares foram informados da violação: ☐ Sim ☐ Não

Hora/Data da comunicação da violação: _____

Forma de comunicação da violação: _____

Número de titulares contactados: _____

Mensagem remetida titulares: _____

7. Medidas Preventivas/Corretivas (a ser preenchido pelo Departamento Responsável Incidentes)

Que medidas foram aplicadas para corrigir/mitigar a violação:

_____

Anexo II – Procedimento de Avaliações Prévias de Impacto

1. Em que consiste a AIPD?

As Avaliações Prévias de Impacto (AIPD) ou *Privacy Impact Assessments* (PIA's), surgem em alternativa às autorizações prévias emitidas pela CNPD, impostas pela Lei 67/98, de 26 de outubro (LPDP) para certos tipos de tratamento de dados pessoais. Encontram-se previstas nos artigos 35º e seguintes do RGPD[1].

A AIPD corresponde a "*um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos. As AIPD's são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento (…). Por outras palavras,* ***uma AIPD é um processo que visa estabelecer e demonstrar conformidade***".

As AIPD's visam estudar sistematicamente novas situações que possam ser suscetíveis de implicar riscos elevados para os direitos e as liberdades das pessoas singulares.

Uma AIPD pode dizer respeito a uma única operação de tratamento de dados ou pode ser utilizada para avaliar múltiplas operações de tratamento que sejam semelhantes em termos de natureza, âmbito, contexto, finalidade e riscos.

2. Quando deve ser efetuada uma AIPD?

Não é obrigatório realizar uma AIPD para todas as operações que envolvam o tratamento de dados pessoais. Só existe obrigação de realizar uma AIPD quando o tratamento for "*suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*" (artigo 35.º, n.º 1 do RGPD)[2].

A AIPD é obrigatória, pelo menos, nos três casos seguintes:

- Quando se proceda a uma avaliação sistemática e completa de dados pessoais, baseada em tratamentos automatizados, incluindo a definição de perfis;
- Quando se tratem categorias especiais de dados (dados relativos a saúde, dados que revelem opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados biométricos, etc.), ou de dados pessoais relacionados com condenações penais e infrações, em grande escala;
- Quando se efetue um controlo sistemático de zonas públicas, em grande escala.

[1] Sigla que designa o Regime Geral da Proteção de Dados. Trata-se da norma jurídica europeia que, complementada por legislação nacional, regula a matéria relativa à proteção das pessoas singulares.

[2] O RGPD impõe assim que "*quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*" o responsável pelo tratamento deve, antes do tratamento, fazer a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

Certo é que o RGPD não é taxativo, i.e, não são apenas as operações supra descritas que carecem de uma AIPD. Mostra-se assim essencial a análise dos seguintes critérios, com vista a se poder concluir se determinada operação pode constituir ou não um elevado risco para os direitos e liberdades das pessoas singulares:

- Avaliação ou classificação: serem tratados aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados.
- Decisões automatizadas: Existirem decisões automatizadas (i.e, sem intervenção humana) que produzam efeitos jurídicos ou afetem significativamente de modo similar o titular dos dados.
- Controlo sistemático: o tratamento ser utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um *"controlo sistemático de zonas acessíveis ao público".*
- Dados especiais ou dados de natureza altamente pessoal: serem tratadas categorias especiais de dados pessoais, tais como dados referentes a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual, bem como dados pessoais relacionados com condenações penais e infrações.
- Operações de tratamento em grande escala: devem ser considerados os seguintes fatores quando se determina se o tratamento é ou não efetuado em grande escala:
  a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
  b. o volume de dados e/ou a diversidade de dados diferentes a tratar;
  c. a duração da atividade de tratamento de dados ou a sua pertinência;
  d. a dimensão geográfica da atividade de tratamento.
- Estabelecer correspondências ou combinar conjuntos de dados que excedam as expectativas razoáveis do titular dos dados.
- Dados relativos a titulares de dados vulneráveis: quando haja um acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, de tal forma que os titulares possam não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos.
- Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais que possam envolver novas formas de recolha e utilização dos dados pessoais recolhidos.
- Quando o próprio tratamento impeça os titulares dos dados "*de exercer um direito ou de utilizar um serviço ou um contrato*".

Analisados todos os referidos critérios, quanto maior o número de critérios for preenchido pela operação que se pretende realizar, maior será a probabilidade de este significar um elevado risco para os direitos e as liberdades dos titulares dos dados e, por conseguinte, de necessitar de uma AIPD, independentemente das medidas de segurança que o responsável pelo tratamento adote.

3. Isenções

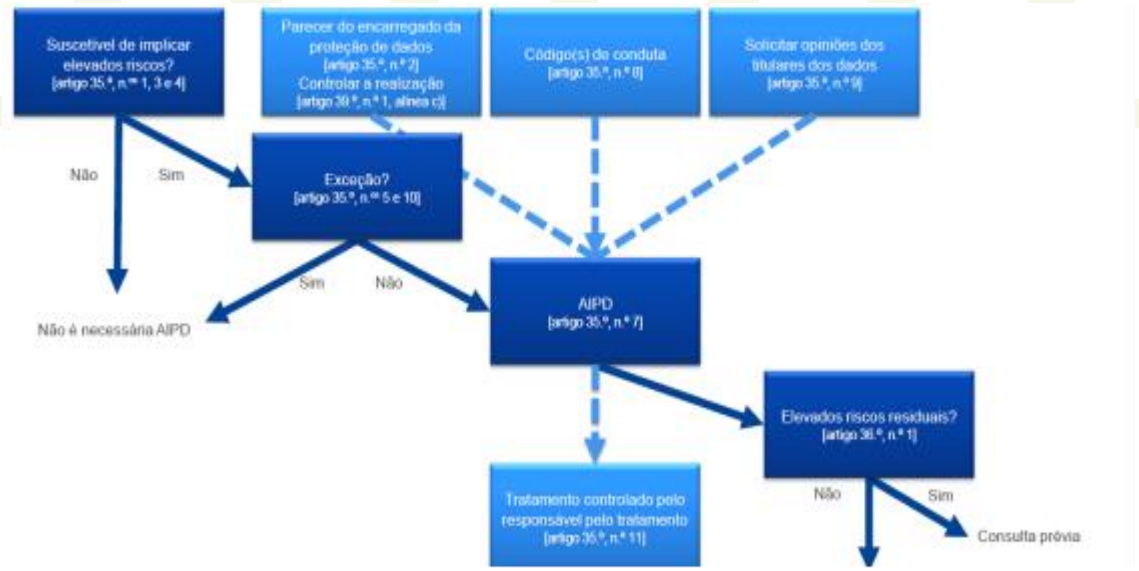
Estão isentos de realização de uma AIPD os seguintes tratamentos:

- Quando o tratamento não for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares;
- Quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada um PIA;
- Quando as operações de tratamento tiverem sido previamente controladas por uma Autoridade de Controlo antes de maio de 2018 em condições específicas que não se tenham alterado;
- Quando uma operação de tratamento tiver um fundamento jurídico no direito da UE ou de um Estado, em que o direito regule a operação de tratamento específica e em que a PIA já tenha sido realizada como parte da adoção desse fundamento jurídico;
- Quando o tratamento estiver incluído na lista opcional (definida pela Autoridade de Controlo) de operações de tratamento para as quais não é obrigatória uma PIA.

4. Como deve ser efetuada uma AIPD?

A AIPD deve ser realizada antes de se iniciar o tratamento de dados pessoais, o mais cedo possível, sendo para tal imprescindível elaborar à partida uma planificação detalhada do tratamento previsto, de modo a que se torne possível fazer uma avaliação da necessidade e proporcionalidade do tratamento em questão.

O esquema seguinte resume as várias fases inerentes a uma AIPD:



Fase 1: **Análise da necessidade de ser efetuada uma AIPD**
Sempre que se equacione a criação de uma nova operação que, de alguma forma ou através de qualquer suporte, importe o tratamento de dados pessoais, deverá ser efetuada preliminarmente uma análise acerca da necessidade ou não de se efetuar uma AIPD.
Para o efeito, deverá começar-se por analisar se a operação em causa consubstancia uma das seguintes operações, que importam obrigatoriamente uma AIPD:

- uma avaliação sistemática e completa de dados pessoais, baseada em tratamentos automatizados, incluindo a definição de perfis;
- o tratamento de categorias especiais de dados, em grande escala;
- o controlo sistemático de zonas públicas, em grande escala.

Afastando-se tais operações, importará ainda analisar os 9 critérios supra descritos em 7.2, por forma a avaliar se a operação que se pretende implementar constitui ou não um elevado risco para os direitos e as liberdades dos titulares dos dados.
No final de tal análise, e dependendo dos resultados, haverá ainda que verificar se está ou não preenchida alguma das causas de isenção da AIPD (7.3).
Findas as três sub-análises desta Fase 1, e concluindo-se que, nos termos do art.35º do RGPD, deve ser efetuada uma AIPD, o processo deverá seguir para as restantes fases.

Fase 2: Análise da operação
A AIPD deverá começar pela análise detalhada dos seguintes itens:

a) Uma descrição sistemática da operação e do tipo de tratamento de dados, devendo destacar-se:
   - A finalidade do tratamento;
   - Os fundamentos de legitimidade para tal tratamento (por exemplo, a execução de um contrato, o cumprimento de uma obrigação legal ou os interesses legítimos do responsável pelo tratamento);
   - A duração de tal operação;
   - Os suportes (físicos ou digitais) nos quais os dados poderão circular;
   - A(s) pessoa(s)/departamento(s) responsável (eis) pela operação.

b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos (explicação do porquê da necessidade do tratamento de dados, efetuando-se um juízo de necessidade e proporcionalidade);

c) Uma avaliação dos riscos para os direitos e liberdades dos titulares – análise de como são assegurados os princípios da confidencialidade, integridade e disponibilidade dos dados pessoais a serem tratados e riscos de poderem não ser assegurados tais princípios; e

d) As medidas previstas para mitigar os riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com os princípios da confidencialidade, integridade e disponibilidade dos dados, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

A previsão destas medidas implica, assim, naturalmente, uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados e a adoção de medidas que deem resposta aos riscos detetados.

Fase 3: Relatório Final

Todos os passos previamente mencionados, bem como as conclusões deles retiradas e medidas adotadas deverão ficar convenientemente documentados num Relatório Final, devendo o mesmo ser sujeito a reavaliações case as operações em causa possam sofrer alterações relativamente ao primeiro modelo estudado.

É essencial não esquecer que a AIPD é um processo contínuo, especialmente quando uma operação de tratamento é dinâmica e está sujeita a mudanças permanentes, pelo que não poderá ser encarado como um exercício único não sujeito a manutenções e atualizações, até porque tal desvirtuaria o seu propósito de instrumento de gestão de risco de violações dos direitos e liberdades dos titulares dos dados e garantia do cumprimento do RGPD.

O esquema seguinte identifica, de forma sintética, os vários passos que devem compor uma AIDP:

5. Que entidades devem ser envolvidas na AIPD?

1. Responsável pelo tratamento

A TURBOMAR, enquanto responsável pelo tratamento é, antes de mais, a responsável por garantir a realização da AIPD. É também à TURBOMAR, que cabe escolher uma metodologia para as AIPD's e garantir a manutenção, atualização e documentação da mesma.

A presente Política pretende espelhar a metodologia que deve ser seguida por cada departamento da TURBOMAR aquando da promoção de uma nova operação que envolva o tratamento de dados pessoais, deverá seguir.

Dependendo do tratamento, a realização da AIPD incumbirá a responsável pela proteção de dados.

2. Subcontratantes

Se o tratamento for total ou parcialmente efetuado por um subcontratante[3], o subcontratante deve auxiliar a TURBOMAR na realização da AIPD e fornecer-lhe todas as informações necessárias. Esta obrigação de auxílio deverá constar do contrato de subcontratação celebrado entre *a TURBOMAR* e cada subcontratante.

3. Autoridade de controlo (Consulta Prévia)

Sempre que da AIPD se concluir que determinado tratamento resultará num elevado risco face à ausência das medidas que possam mitigar tais riscos, recomenda-se que a Autoridade de Controlo (CNPD) deva ser previamente consultada (procedimento de Consulta Prévia).
Aquando de tal consulta, devem ser prestados os seguintes esclarecimentos:

a) A repartição de responsabilidades com outros responsáveis pelo tratamento ou subcontratantes envolvidos no tratamento, nomeadamente no caso de um tratamento dentro de um grupo empresarial (se aplicável);
b) As finalidades e os meios do tratamento previsto;
c) As medidas e garantias previstas para defesa dos direitos e liberdades dos titulares dos dados nos termos do presente regulamento;
d) O resultado da AIDP realizada;
e) Quaisquer outras informações solicitadas pela Autoridade de Controlo.

Face a tal Consulta Prévia, a Autoridade de Controlo, no prazo máximo de 8 semanas a contar da receção do pedido de consulta, deverá em emitir a sua decisão final quanto à operação cuja consulta foi apresentada.

6. Análise de resultados e consequências

Conforme foi já referido, a AIPD é um processo contínuo, pelo que qualquer AIPD efetuada deve ser obrigatoriamente documentada. Nesse sentido, toda a documentação recolhida e preparada ao longo de uma AIPD, deverá ser guardada na Direção Financeira
Regularmente deverá a responsável pela proteção de dados, proceder a um controlo posterior para avaliar se o tratamento é realizado em conformidade com as conclusões retiradas, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam.

[3] Sobre os Subcontratantes consulte o capítulo "*Entidades Relacionadas*".

Anexo III – Formulários com modelos de recolha de dados pessoais

Modelo 1 – Requerimento interno de dados pessoais de colaboradores
(RGPD M 001 V 2019.001)

Modelo 2 – Declaração de comunicação de dados pessoais
(RGPD M 002 V 2019.001)

Modelo 3 – Aditamento ao contrato de Prestação de Serviços
(RGPD M 003 V 2019.001)

Requerimento interno de dados pessoais de colaboradores

A Área _____-, solicita aos Recursos Humanos os seguintes dados pessoais do (s) trabalhador (s) :

	Mapa da Segurança Social
	EPI (Ficha de equipamentos de proteção individual)
	Ficha de Aptidão Médica
	Nº do cartão do cidadão
	NIF – Número de Identificação Fiscal
	Data de nascimento
	Passaporte de Segurança
	Outro

Finalidade: Trabalhos para_____

no dia _____, os quais serão eliminados logo após o término dos trabalhos.

O colaborador: _____

Data: _____/_____/_____

Grupo Turbomar

Sede
Rua da Garagem, 8
2790-078 Carnaxide
Portugal
Tel.: +351 214 168 410
Fax: +351 214 168 411

Delegação Norte
Rua Industrial da Mina, 73
4410-269 Canelas VNG
Portugal
Tel.: +351 223 743 656
Fax: +351 223 743 658

Delegação Sul
Armazém 4 - Abelheira
8100-060 Boliqueime
Portugal
Tel.: +351 289 170 510

E-mail: info@turbomar.pt
URL: www.turbomar.pt

Declaração

A entidade xxxxxx declara que todos os dados pessoais (nomeadamente dados de trabalhadores) que lhe sejam comunicados pela Turbomar Energia, Lda para efeitos de execução e gestão do contrato celebrado entre as duas entidades, serão tratados no estrito respeito pela legislação aplicável à proteção de dados pessoais, comprometendo-se a adotar as medidas técnicas e organizativas necessárias para assegurar a integralidade e confidencialidade dos dados que lhe sejam cedidos.

Mais se compromete**,** a não proceder à transmissão dos dados entregues, a subcontratantes ou entidades terceiras, sem o consentimento prévio e expresso da Turbomar Energia, Lda e, logo que cesse a finalidade para a qual o tratamento é realizado (e.g. fim da relação contratual), a eliminar ou devolver à Turbomar Energia, Lda., todos os dados pessoais que lhe tenham sido transmitidos.

Data e local:

Assinatura e carimbo

Grupo Turbomar

Sede
Rua da Garagem, 8
2790-078 Carnaxide
Portugal
Tel.: +351 214 168 410
Fax: +351 214 168 411

Delegação Norte
Rua Industrial da Mina, 73
4410-269 Canelas VNG
Portugal
Tel.: +351 223 743 656
Fax: +351 223 743 658

Delegação Sul
Armazém 4 - Abelheira
8100-060 Boliqueime
Portugal
Tel.: +351 289 170 510

E-mail: info@turbomar.pt
URL: www.turbomar.pt

Aditamento ao contrato de Prestação de Serviços

Entre:
Turbomar Energia – Equipamentos de Produção e Serviços de Assistência, Lda, com sede na Rua da Garagem nº 8, 2790-078 Carnaxide, pessoa coletiva nº 500290946, com o capital social de € 1.320.200,00 (um milhão trezentos e vinte mil e duzentos euros), representada por Maria Eugénia da Silva Morais Dahlin, na qualidade de Sócia-Gerente, com poderes para o ato, em conformidade com a certidão permanente com o código 0105-1765-2458, adiante designada de Primeira Contraente.
E
(Nome Cliente) com sede na Rua _____, xxxx-xx (Localidade), pessoa coletiva nº xxxxxxxx, com o capital social de €_____(extenso) , representada por X, na qualidade de (administrador ou gerente), com poderes para o ato, em conformidade com a certidão permanente com o código XXXX-XXXX-XXXX-XXXX, adiante designada de Segunda Contraente.

Conjuntamente designadas por "Partes"

CONSIDERANDO QUE:
a) As Partes celebraram em (data), um contrato de prestação de serviços (doravante designado de contrato) com o nº G0XXXXX;
b) Em conformidade com a nova regulamentação de proteção de dados, nomeadamente o regulamento (UE) de 2016/679, do Parlamento Europeu do Conselho de 27 de abril de 2016, acordam as partes aditar nova cláusula ao contrato;
c) Todo o restante clausulado do contrato manter-se-á em vigor.

Acordam as partes na celebração do presente aditamento ao contrato de prestação de serviços, que se rege pelos considerandos supra e pela cláusula seguinte:

Cláusula 1
Proteção de Dados

Para efeitos de execução do presente contrato de assistência técnica, caso qualquer uma das Partes aceda a dados pessoais da respetiva contraparte (nomeadamente dos seus representantes ou colaboradores), obriga-se a tratar tais dados unicamente para efeitos de gestão desta prestação de serviços e em respeito pelos princípios e obrigações impostas pela legislação nacional e comunitária referente ao tratamento de dados pessoais.

As alterações formalizadas pelo presente aditamento entrarão em vigor na data da sua assinatura.

Celebrado (Data), em dois exemplares, ficando um para cada Partes.

Primeira Contraente — Segunda Contraente

_____ — _____

(Nome) — (Nome)

Grupo Turbomar

Sede
Rua da Garagem, 8
2790-078 Carnaxide
Portugal
Tel.: +351 214 168 410
Fax: +351 214 168 411

Delegação Norte
Rua Industrial da Mina, 73
4410-269 Canelas VNG
Portugal
Tel.: +351 223 743 656
Fax: +351 223 743 658

Delegação Sul
Armazém 4 - Abelheira
8100-060 Boliqueime
Portugal
Tel.: +351 289 170 510

E-mail: info@turbomar.pt
URL: www.turbomar.pt