REGULAMENTO DE PROTECÇÃO DE DADOS PESSOAIS

OS 03/2024

Caixa Angola
Banco Caixa Geral Angola

ÍNDICE

1. INTRODUÇÃO

A conformidade com a Lei da Protecção de Dados, aplicável plenamente aos 17.06.2011, implica a adopção de políticas, práticas e procedimentos pelas empresas e organizações a ela sujeita.

O Grupo CGD tem vindo a adaptar-se com vista a assegurar a conformidade no domínio da protecção dos dados pessoais, *maxime*, o "RGPD", no caso em concreto do BCGA conjuga-se com a "LPD".

O Modelo de Governo da Protecção de Dados visa operacionalizar a Política de Protecção de Dados Pessoais e a Política de Privacidade e de Protecção de Dados Pessoais através da definição do modelo de governo interno e da atribuição de responsabilidades e directrizes de alto nível sobre a matéria aos intervenientes identificados, consagrando métodos de monitorização e reporte institucional sobre protecção de dados, bem como os fora de comunicação regular e urgente nesta matéria.

Dentro do ciclo de gestão, os processos específicos de protecção de dados relativos ao inventário de finalidades de tratamento de dados pessoais, à avaliação de impacto sobre a protecção de dados pessoais (DPIA), às situações de violação de dados pessoais, a resposta aos direitos dos titulares, a emissão de pareceres e recomendações pelo *Data Protection Officer* e o acompanhamento das Entidades CGD são detalhados, atenta a necessidade de clarificar as responsabilidades dos respectivos intervenientes, inclusive através de outros normativos internos.

O presente normativo define o ciclo de gestão da protecção de dados, que assegura a existência de mecanismos de monitorização e reporte periódico, com o intuito de favorecer uma cultura de melhoria contínua da gestão da protecção de dados.

É ainda estabelecido o modelo de comunicação e acompanhamento do BCGA, fomentando a cooperação constante e a comunicação com o *Data Protection Officer* corporativo.

2. OBJECTO

O presente normativo visa assegurar a operacionalização da Política de Protecção de Dados Pessoais e a Política de Privacidade e de Protecção de Dados Pessoais (divulgadas no SNI e no site do BCGA) através da definição do regulamento interno que identifica os intervenientes, estabelece responsabilidades e directrizes de alto nível sobre a protecção de dados, e define o ciclo de gestão de protecção de dados e os processos específicos dessa gestão.

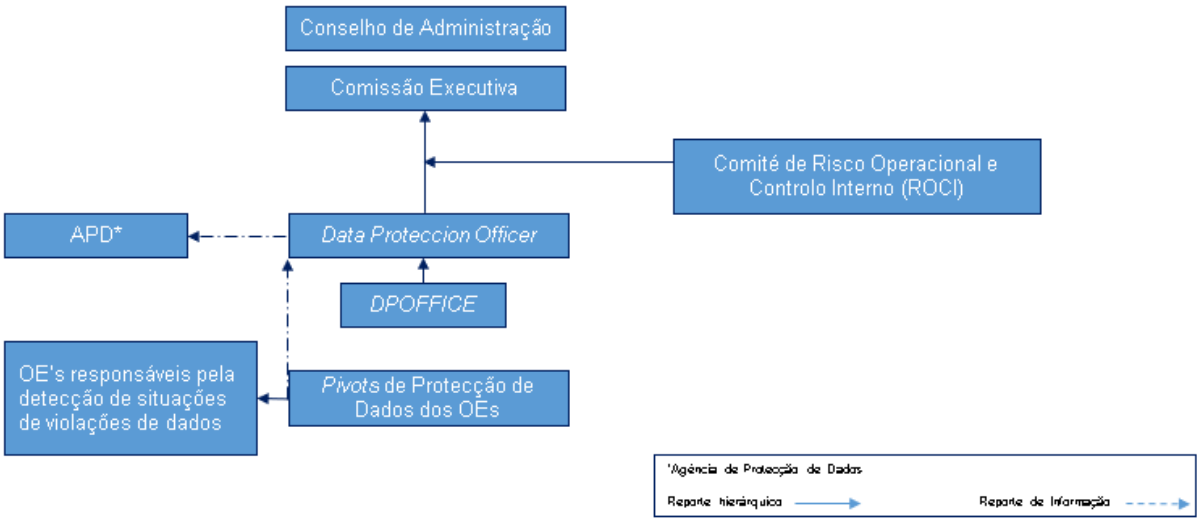
O Regulamento da Protecção de Dados Pessoais, consagra os métodos e os mecanismos de monitorização e reporte periódico institucional sobre protecção de dados, bem como os fora de comunicação regular e urgente nesta matéria, com o intuito de favorecer uma cultura de melhoria contínua da gestão da protecção de dados.

Complementarmente, o presente normativo define o modelo de comunicação e acompanhamento do BCGA, fomentando a cooperação constante e a comunicação com o *Data Protection Officer* corporativo.

3. ESTRUTURA E ORGANIZAÇÃO NO BCGA

A protecção de dados é uma responsabilidade individual de todos os Colaboradores do BCGA, bem como dos membros dos seus órgãos de administração, nas funções de gestão e de fiscalização.

Além dos respectivos colaboradores, intervêm no ciclo de gestão de dados pessoais o Órgão de Administração, a Comissão Executiva, o Comité de Risco Operacional e Controlo Interno (ROCI), o *Data Protection Officer*, a *Data Protection Office*, os Directores de primeira linha do BCGA, os *Pivots* de Protecção de Dados dos Órgãos de Estrutura do BCGA.



As responsabilidades de cada interveniente são as seguintes:

3.1. Comissão Executiva do BCGA

3.1.1. Os membros da Comissão Executiva do BCGA obrigam-se a cumprir os princípios, regras e procedimentos respeitantes à Política de Protecção de Dados Pessoais, cabendo-lhes assegurar a conformidade legal em matéria de protecção de dados e implementar as estruturas e garantir os recursos adequados para assegurar essa conformidade.

3.1.2. Compete à Comissão Executiva:

a) Definir as políticas sobre protecção de dados e garantir que a estrutura e a cultura organizacionais permitam desenvolver adequadamente a estratégia definida nesse domínio;

b) Nomear o *Data Protection Officer* - encarregado de protecção de dados – e instituir o *Data Protection Office*, assegurando que a função de protecção de dados tem autoridade necessária para desempenhar as respectivas competências de forma objectiva e independente, tem acesso a toda a informação necessária e relevante e que o Órgão de Estrutura onde se insere organicamente o *Data Protection Office* proporciona os recursos materiais e humanos adequados ao desempenho das respectivas tarefas;

c) Comunicar à autoridade de controlo o início e a cessação das funções do *Data Protection Officer*;

d) Aprovar o Orçamento, o Plano de Actividades, o Relatório de Actividades e o Plano de Formação do *Data Protection Office*, assegurando que estão criadas as condições para o cumprimento pleno da missão conferida ao *Data Protection Officer*;

e) Aprovar políticas e procedimentos concretos, eficazes e adequados, para a identificação, avaliação, acompanhamento e controlo dos riscos a que o BCGA está exposto em matéria de protecção de dados, assegurando a sua implementação e cumprimento;

f) Verificar regularmente, com periodicidade mínima anual, o cumprimento das políticas e procedimentos de gestão de dados pessoais, avaliando a sua eficácia e contínua adequação à actividade, conferindo-se especial atenção a eventuais alterações dos factores internos e externos que afectem o BCGA, no sentido de possibilitar a detecção e correcção de quaisquer deficiências;

g) Apreciar e aprovar os relatórios elaborados pelo *Data Protection Officer;*

h) Envolver o *Data Protection Officer* em tempo útil e de forma adequada em todas as questões relacionadas com os dados pessoais;

i) Assegurar que todos os Colaboradores compreendem o seu papel na gestão da protecção de dados pessoais de forma a poderem contribuir de forma efectiva para o cumprimento e a cultura organizacional de protecção de dados;

j) Promover uma cultura organizacional de protecção de dados no BCGA.

3.2 Órgão de Administração ou de Gestão de topo do BCGA

Os Órgãos de Administração ou de Gestão de topo do BCGA são responsáveis por garantir que a protecção de dados pessoais está incorporada, desde a fase embrionária, em todo o ciclo da actividade do BCGA, tendo para tal as seguintes responsabilidades:

a) Nomear o *Data Protection Officer,* a quem compete a coordenação da gestão do risco de conformidade sobre protecção de dados, preferencialmente da área congénere à Direção de Organização e Qualidade, podendo acumular com outras funções não incompatíveis, definindo, por meio de normativo interno, responsabilidades, autonomia, independência e funções;

b) Garantir a segregação de funções e a prevenção de conflitos de interesses;

c) Assegurar a existência de um sistema de controlo que inclua a implementação de circuitos de comunicação aos *Data Protection Officer* de quaisquer indícios de situações de incumprimento de obrigações legais, de regras de conduta e de relacionamento com clientes e outros titulares de dados, bem como de outros deveres abrangidos pelo risco de conformidade sobre protecção de dados;

d) Garantir que são disponibilizados os recursos humanos, materiais e tecnológicos necessários e suficientes para o desempenho efectivo das responsabilidades ao *Data Protection Officer;*

e) Assegurar que é ministrada formação sobre protecção de dados pessoais ao *Data Protection Officer*, bem como a todos os Colaboradores que tratem dados pessoais no âmbito das suas responsabilidades funcionais;

f) Garantir a transposição dos normativos corporativos relativos à protecção de dados;

g) Garantir reporte ao *Data Protection Officer* corporativo;

h) Tomar conhecimento e acompanhar os relatórios elaborados pelo *Data Protection Officer* com impacto no BCGA, nomeadamente os que incluam recomendações para a adopção de medidas correctivas.

3.3 *Data Protection Officer do BCGA*

No BCGA, a conformidade sobre protecção de dados é assegurada de forma independente e encabeçada pelo *Data Protection Officer*, que assegura, em estreita articulação com o *Data Protection Officer* corporativo, a coordenação da gestão da protecção de dados.

Para tal, têm atribuídas as seguintes responsabilidades:

a) Controlar, de forma permanente, independente e efectiva, o cumprimento das obrigações legais, de conduta e de outros deveres aplicáveis em matéria de protecção de dados pelo BCGA;

b) Acompanhar e avaliar regularmente a adequação e eficácia das medidas e procedimentos adoptados pelo BCGA para detectar qualquer risco de incumprimento das obrigações legais e deveres a que se encontra sujeita em matéria de protecção de dados, bem como das medidas tomadas para corrigir eventuais deficiências no respectivo incumprimento;

c) Garantir a transposição para normativo interno da legislação e regulamentação aplicáveis, bem como a adaptação e/ou adopção de normativos internos transversais e de âmbito corporativo;

d) Prestar toda a colaboração ao *Data Protection Officer* corporativo e dar-lhe acesso à documentação necessária ao exercício das suas atribuições funcionais;

e) Submeter à apreciação do *Data Protection Officer* corporativo a aprovação do Plano de Actividades e do Relatório anual de actividades;

f) Informar o *Data Protection Officer* corporativo das situações de não conformidade detectadas, incluindo as notificações a efectuar à autoridade de controlo competente e as comunicações aos titulares dos dados quando as violações de dados pessoais forem susceptíveis de implicar elevado risco para os direitos e liberdades dos titulares;

g) Documentar os ciclos de gestão de protecção de dados pessoais, especialmente os referentes aos processos específicos relativos ao Inventário de finalidades de tratamento, à avaliação de impacto sobre a protecção de dados pessoais (DPIA), à violação de dados pessoais, a resposta aos direitos dos titulares, a emissão de pareceres e a sua articulação e cooperação com o *Data Protection Officer* corporativo;

h) Elaborar e manter actualizado um repositório relativo às avaliações de impacto sobre a protecção de dados e as situações de violação de dados pessoais, notificadas à autoridade de controlo e comunicadas aos titulares dos dados;

i) Garantir o acompanhamento da implementação e a monitorização contínua da actividade da Entidade do ponto de vista da conformidade sobre protecção de dados;

j) Gerir as respectivas equipas de apoio de protecção de dados e assegurar os processos equivalentes aos *supra* identificados para o *Data Protection Office*.

k) Coordenar funcionalmente os Pivots de Protecção de Dados dos vários OE do BCGA, no âmbito da gestão do risco de conformidade sobre protecção de dados

3.3.1 O parecer do *Data Protection Officer* tem carácter consultivo, devendo, contudo, o responsável específico do processo de tratamento de dados fundamentar a eventual posição em sentido contrário, submetendo, para decisão, à Comissão Executiva.

3.3.2. O *Data Protection Officer* deve ser informado de toda e qualquer comunicação com as autoridades de controlo (nacional e estrangeiras) sobre protecção de dados, sendo obrigação dos demais Órgãos de Estrutura realizar, sempre que pertinente (i.e, quando exista um risco de desconformidade com a LPD), um pedido de parecer prévio ao *Data Protection Officer* no sentido de:

a) garantir a pertinência da comunicação;

b) assegurar a consistência com comunicações anteriores;

c) validar que a comunicação em questão não se enquadra no âmbito das responsabilidades estabelecidas pelo *Data Protection Officer* no seu modelo funcional.

3.4 *Data Protection Office*

A *Data Protection Office* tem por missão prestar, colaboração e assistência institucional ao *Data Protection Officer* no exercício das suas funções, de quem dependem.

3.5 Directores de primeira linha de Órgãos de Estrutura do BCGA

A responsabilidade dos Directores de primeira linha dos Órgãos de Estrutura do BCGA, no âmbito da gestão da protecção de dados, abrange as seguintes actividades:

a) Implementar, no âmbito da actividade sob sua responsabilidade, os procedimentos de controlo que se revelem adequados para a mitigação do risco de protecção de dados associado à actividade desenvolvida;

b) Garantir que no momento de definição dos meios de tratamento e no próprio tratamento são asseguradas medidas técnicas e organizativas adequadas destinadas a aplicar com eficácia os princípios de protecção de dados e que por defeito só são tratados os dados pessoais que sejam necessários para cada finalidade específica de tratamento;

c) Nomear um Colaborador como *Pivot* de Protecção de Dados para coordenação da gestão da protecção de dados na estrutura de negócio;

d) Assegurar que é disponibilizado ao *Pivot* de Protecção de Dados o tempo necessário ao exercício desta função;

e) Fundamentar, enquanto responsável pelo tratamento de dados, a decisão discordante do parecer emitido pelo *Data Protection Officer*;

f) Fornecer e facilitar o acesso à informação necessária ao desenvolvimento das actividades do *Data Protection Officer* e dos Colaboradores do *Data Protection Office*.

3.6 Órgãos de Estrutura envolvidos nos processos específicos do ciclo de gestão de dados:

3.6.1 Sem prejuízo das responsabilidades inerentes aos processos específicos do ciclo de gestão de protecção de dados atribuídas no ponto IV deste normativo, compete aos Órgãos de Estrutura envolvidos[1]:

a) Conceber e implementar medidas de fundamentação legal relativas às finalidades de tratamento inventariadas, bem como relativas à resposta a vulnerabilidades detectadas, com recurso ao GAJ, se necessário;

b) Adoptar as medidas de mitigação de risco no âmbito de uma avaliação de impacto sobre os direitos e liberdades dos titulares dos dados (DPIA);

[1] Ver, infra, gráfico do ciclo de gestão da protecção de dados (ponto IV).

c) Adoptar as medidas preventivas e reactivas para a eficiente gestão de violações de dados pessoais;

d) Solicitar ao *Data Protection Officer* os pedidos de esclarecimentos e emissão de parecer e/ou recomendações no âmbito da protecção de dados;

e) Assegurar a resposta aos direitos dos titulares dos dados, em articulação com as orientações do *Data Protection Officer* e os procedimentos organizativos internos adoptados para o efeito;

f) Colaborar activamente com o *Data Protection Officer*, dando-lhe acesso e facultando-lhe todos os documentos e informações relevantes para o exercício das suas funções.

3.6.2. Compete aos Órgãos de Estrutura, em articulação com o *Data Protection Officer*, assegurar:

a) A actualização do inventário de finalidades de tratamento;

b) A utilização da versão mais actualizada da metodologia de DPIA;

c) A gestão de eventos de violação de dados pessoais;

d) A operacionalização dos mecanismos e procedimentos de resposta que garantam o exercício dos direitos dos titulares dos dados.

3.7 *Pivots* de Protecção de Dados dos Órgãos de Estrutura do BCGA

3.7.1. Os *Pivots* de Protecção de Dados do BCGA apoiam os Directores de primeira linha dos Órgãos de Estrutura do BCGA, coordenando as actividades de gestão da protecção de dados nas respectivas estruturas.

São os interlocutores privilegiados com o *Data Protection Officer*, particularmente no que se refere à identificação, avaliação, acompanhamento e controlo dos riscos de protecção de dados que emanam da legislação em vigor e de outros deveres aplicáveis às áreas de negócio e de actividades respectivas.

3.7.2. Para tal, têm atribuídas as seguintes responsabilidades, em estreita colaboração com o *Data Protection Office*:

a) Controlar, de forma permanente e efectiva, o cumprimento das obrigações legais, de conduta e de outros deveres aplicáveis sobre protecção de dados ao Órgão de Estrutura;

b) Assegurar a identificação das situações de risco de protecção de dados e respectivas medidas mitigadoras, garantindo o acompanhamento da implementação das mesmas e a monitorização contínua da actividade do Órgão de Estrutura do ponto de vista da conformidade sobre protecção de dados;

c) Comunicar ao *Data Protection Officer*, com conhecimento do Director de primeira linha do respectivo Órgão de Estrutura, as situações de não conformidade detectadas sobre protecção de dados, bem como as respectivas acções correctivas adoptadas, sem prejuízo do reporte ao Gabinete de Suporte à Função *Compliance*, em observância das normas internas sobre registo de incumprimentos.

3.8 Órgãos de decisão em matéria de protecção de dados no BCGA

O Comité de Risco Operacional e Controlo Interno (ROCI) é órgãos de decisão no que respeita ao acompanhamento e monitorização da conformidade do BCGA em matéria de protecção de dados.

3.9 Comissão Executiva

A Comissão Executiva é informada das violações de dados pessoais notificadas à APD em 72 horas, após conhecimento da violação e comunicadas aos titulares dos dados susceptíveis de implicar risco elevado para os direitos e liberdades das pessoas singulares.

3.10 Comité de Risco Operacional e Controlo Interno (ROCI)

O Comité de Risco Operacional e Controlo Interno (ROCI) regulado pela OS 27/2018, tem as seguintes competências delegadas em matéria de Protecção de Dados:

a) Aprovar o Plano anual de actividades de Protecção de Dados;
b) Analisar o relatório de acompanhamento da protecção de Dados (BCGA), e o relatório anual de Protecção de Dados;
c) Tomar decisões com impacto material para o BCGA como “responsável pelo tratamento”, bem como sobre a gestão da protecção de dados;
d) Acompanhar a evolução da conformidade do BCGA com a LPD e subsidiariamente o RGPD;

e) Suportar a resolução de conflitos e assegurar o *enforcement* necessário para o cumprimento do da LPD e subsidiariamente o RGPD;
f) Definir e acompanhar grupos de trabalho para temas específicos;
g) Aprovar o relatório de acompanhamento da Protecção de Dados (BCGA).

4. CICLO DE GESTÃO

A gestão da protecção de dados pessoais é transversal à Instituição, sem prejuízo da intervenção e responsabilidade de determinados interlocutores e Órgãos de Estrutura, como a seguir melhor se explicita através da matriz de responsabilidades (RACI) constante do Anexo I.

No ciclo de gestão de protecção de dados pessoais, assumem particular destaque pelos impactos na actividade do BCGA os seguintes processos específicos que envolvem a colaboração e co-responsabilidade dos Órgãos de Estrutura definidos no ponto anterior, sem prejuízo de outros cuja intervenção casuística poderá ser crítica para assegurar a melhor defesa da instituição:

- Inventário de finalidades de tratamento de dados pessoais (Registo);
- Avaliação de impacto sobre a protecção de dados pessoais (DPIA);
- Violação de dados pessoais;
- Resposta aos direitos dos titulares;
- Emissão de pareceres;
- Acompanhamento do BCGA pela CGD.

A monitorização e reporte integram também o ciclo de gestão da protecção de dados.

4.1 Processos específicos que integram o ciclo de gestão de protecção de dados

4.1.1. Registo: Inventário de Finalidades de Tratamento (IFT) no BCGA

Para assegurar a conformidade com a LPD e RGPD, o BCGA constituiu um inventário com base nas finalidades de tratamento consideradas no âmbito das autorizações outorgadas pela LPD e CNPD[2], sujeito a actualização frequente que permita assegurar o cumprimento dos requisitos legais aplicáveis.

Foi desenvolvido o 'Questionário de Inventariação de Finalidades de Tratamento de Dados Pessoais' ("QIFT-DP"), que tem por objectivo identificar, para cada finalidade de tratamento de dados pessoais subjacente à actividade do BCGA, quais as categorias de dados pessoais utilizadas, para que categorias de titulares de dados e de que forma são tratados, em conformidade com as pertinentes disposições legais[3].

Os Órgãos de Estrutura são responsáveis por informar o *Data Protection Officer*, de forma proactiva, sempre que verifiquem a necessidade de actualização dos QIFT-DP.

Sem prejuízo das soluções a consagrar em normativo interno específico que regule esta matéria, por forma a manter o 'Inventário de Finalidades de Tratamento' ("IFT") constantemente actualizado, adoptar-se a implementação de um processo semestral, que deverá ser apresentado ao *Data Protection Officer* até 30 de Abril e 30 de Setembro de cada ano, dividido nas seguintes fases:

Preenchimento do QIFT-DP; Incorporação no Inventário; Análise das bases legais; Identificação de vulnerabilidades; Definição de acções e Monitorização de acções.

4.1.1.1. Preenchimento do QIFT-DP

Para efeito da actualização do Inventário, o *Data Protection Officer* enviará, no início dos meses de Março e de Agosto de cada ano, a todos os Órgãos de Estrutura que realizem algum tipo de tratamento de dados pessoais ou que já tenham sido identificados como responsáveis por finalidades de tratamento de dados pessoais, a versão mais recente do questionário.

O questionário será enviado ao *Pivot* de Protecção de Dados identificado por cada Órgão de Estrutura, com conhecimento ao respectivo Director de primeira linha, sendo desejável o envolvimento dos Colaboradores que anteriormente já tenham intervindo em diligências prévias neste âmbito.

Uma vez preenchido, o *Pivot* de Protecção de Dados, com conhecimento do respectivo Director de primeira linha, envia o *Data Protection Office* o(s) questionário(s).

[2] Cf., designadamente a Autorização n.º 2997/2015, aplicável ao BCGA por via da CGD.
[3] Cf. art. 30.º do RGPD, aplicável ao BCGA por via da CGD.

4.1.1.2. Incorporação no IFT

O *Data Protection Officer* validará previamente o grau de completude e qualidade das respostas recebidas através do QIFT-DP e, quando aprovados, a sua incorporação no IFT. A não conformidade das respostas recebidas da parte dos Órgãos de Estrutura implica a sua devolução ao respectivo Órgão de Estrutura para verificação e correcção necessárias a assegurar a conformidade com o pedido.

4.1.1.3. Análise de Bases Legais

O *Data Protection Officer,* com o apoio do *Data Protection Office,* analisa os fundamentos legais documentados pelos Órgãos de Estrutura via QIFT-DP (ex. para recolha e demais operações de tratamento, ou transferência para países terceiros) para aferir se os mesmos são suficientes e adequados a assegurar a conformidade com LPD. Caso necessário, os Órgãos de Estrutura obtêm parecer da Gabinete de Assessória Jurídica (GAJ) de forma a garantir a licitude de todos os tratamentos de dados pessoais realizados no BCGA, antes do envio do QIFT-DP ao *Data Protection Officer*.

4.1.1.4. Identificação de Vulnerabilidades

Complementarmente à análise dos fundamentos de licitude, com base na avaliação da resposta sobre a forma como os dados pessoais são tratados no contexto de uma determinada finalidade, será tido em conta o 'Indicador de Risco sobre Dados Pessoais ("IRDP"), apresentado no IFT com base nos diversos *triggers* de risco recolhidos via QIFT-DP (ex. tratamento de dados de menores – responsabilidades parentais), que destaca as finalidades onde os dados pessoais se encontram mais vulneráveis.

4.1.1.5. Definição de Acções

Com base na identificação de lacunas na fundamentação legal e/ou vulnerabilidades operacionais serão organizadas sessões de trabalho com os Órgãos de Estrutura responsáveis e outros que se considerem relevantes para a discussão, onde seja feita uma análise detalhada do problema e, caso aplicável, decididas acções a tomar que visem a fundamentação legal (ex. recolha de consentimento) e/ou mitigação do risco (medidas de segurança adicionais).

4.1.1.6. Monitorização de Acções

O *Data Protection Officer* e o *Data Protection Office* devem manter um acompanhamento e monitorização constante sobre as acções em execução resultantes do ponto anterior.

Todo o processo de Inventariação das Finalidades de Tratamento deve ser documentado, assegurando-se a existência do respectivo repositório, a fim de poder ser evidenciado à APD, caso seja necessário.

Todo o processo de Inventariação das Finalidades de Tratamento deve ser documentado a fim de poder

4.1.2. Avaliação de impacto sobre a protecção de dados pessoais (DPIA)

4.1.2.1. A avaliação de impacto sobre a protecção de dados pessoais (DPIA) tem como objectivo auxiliar o responsável pelo tratamento na avaliação e mitigação preventiva dos eventos de risco sobre a privacidade de dados (direitos e liberdades das pessoas singulares), com base numa análise custo-benefício entre os recursos necessários para a sua execução e a exposição dos dados pessoais em causa.

O responsável directo pelo tratamento, ou seja, o Órgão de Estrutura que pretende realizar a criação/revisão ao(s) produto(s)/serviço(s), processo(s) ou nova(s) tecnologia(s)/sistema(s) informático(s) ("Órgãos de Estrutura responsáveis"), deve identificar a necessidade de realizar um DPIA.

Os envolvidos no processo de criação/revisão, internos e/ou externos, deverão ser consultados por iniciativa do responsável pelo tratamento, com o intuito de utilizar os seus conhecimentos do processo para ajudar na identificação de fluxos de dados, riscos associados e possíveis medidas de mitigação. Esta contribuição pode ser dada através de várias vias e independentemente do estágio da criação/revisão em análise.

O *Data Protection Officer* deverá ser notificado sempre que se dê início a um DPIA, sendo consultado quando necessário para que o Órgão de Estrutura seja capaz de concretizar a aplicação da metodologia.

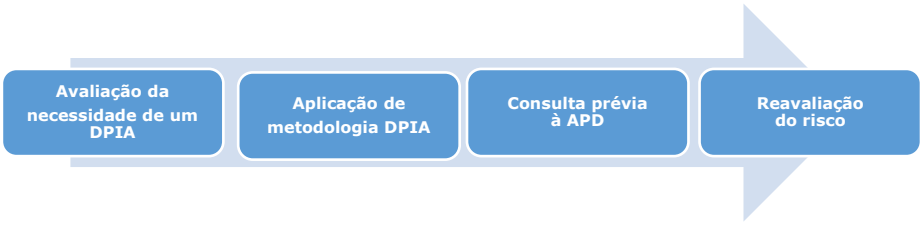
Posteriormente, o envolvimento do *Data Protection Officer* é particularmente relevante sempre que o risco é suficientemente elevado para desencadear um processo de consulta prévia à APD.

Deve ser considerada a consulta dos titulares dos dados (ex. *focus group*) sempre que relevante, informando-os sobre os tratamentos novos/revistos aos seus dados, aferindo a sua aceitação sobre os mesmos e solicitando a sua contribuição na identificação de riscos e das medidas ou preferências que considerem pertinentes para a sua salvaguarda.

Ao ser envolvido num DPIA, o *Data Protection Officer* pode sugerir adaptações específicas à metodologia transversal, ajudando o Órgão de Estrutura responsável pelo tratamento a maximizar a eficiência do processo. Paralelamente, a sua participação deverá ter como intuito melhorar a qualidade da avaliação

do risco, a definição do nível de risco residual aceitável e a partilha de conhecimentos específicos, nomeadamente sobre o LPD, que agreguem conteúdo e profundidade à análise.

4.1.2.2. Processo de avaliação de impacto sobre a protecção de dados (DPIA)



Avaliação da necessidade de um DPIA

A análise de um conjunto de operações de tratamento e averiguação da necessidade de um DPIA deve ser considerada sempre que uma actividade - nova ou estruturalmente revista - de utilização de dados pessoais for pensada, alertando previamente a DPO para possíveis impactos que esta poderá ter na garantia do cumprimento da Política de Protecção de Dados Pessoais e, sobretudo, da LPD e outros requisitos regulatórios aplicáveis. Para efeito da avaliação da necessidade de realizar um DPIA, ver o questionário (Anexo II).

Dependendo do grau de profundidade a aplicar, o processo pode ser executado faseadamente, sempre considerando a primeira data possível e numa fase de desenho funcional e/ou técnico do novo tratamento, como medida de prevenção. Não obstante a incorporação do DPIA nos processos existentes de desenvolvimento e revisão de produtos/serviços, processos e tecnologias/sistemas, o alerta da possível necessidade de análise deve ser indicado pelos Órgãos de Estrutura directamente envolvidos no tratamento de dados da actividade, entrando em contacto com o *Data Protection Officer*.

Actividades

Cabe ao Órgão de Estrutura em causa caracterizar o projecto, nomeadamente identificando as finalidades subjacentes, fundamentos de licitude, categorias de dados tratadas, número de titulares potencialmente afectados e tecnologias/ sistemas informáticos utilizados (entre outra informação pertinente sobre o tratamento de dados pessoais e risco potencialmente envolvido no mesmo);

Para o efeito, o formulário (Anexo II) deve ser preenchido pelo Órgão de Estrutura enquanto responsável pelo tratamento neste processo específico do ciclo de gestão de dados pessoais, para levantamento geral das principais características das operações previstas – nomeadamente se existe a necessidade de recolha de dados adicionais ou tratamento para novas finalidades, envolvimento de novas áreas/entidades ou utilização de meios potencialmente intrusivos. Este documento de avaliação preliminar de risco deve identificar particularmente situações que impliquem:

- Tratamento para fins de avaliação ou *scoring* de pessoas singulares;
- Tratamento como base para tomada de decisões automáticas que produzam efeitos significativos na esfera jurídica do titular dos dados (ex. como *profiling*);
- Tratamento em larga escala (i.e. elevado, volume de dados, número de titulares afectados, longa duração ou abrangência geográfica);
- Monitorização sistemática de pessoas singulares (ex. em áreas públicas);
- Tratamento de dados sensíveis (ex. dados biométricos, médicos, legais);
- Tratamento de dados relativos a pessoas singulares em situações de vulnerabilidade (como Colaboradores, indivíduos incapacitados, menores);
- Utilização de dados que foram correspondidos ou combinados, provenientes de duas ou mais fontes e/ou operações de tratamento de dados;
- Recurso a novas soluções tecnológicas que ainda não se encontrem em utilização na organização;
- Transferência de dados pessoais para fora do Espaço Económico Europeu;
- Dificuldade dos titulares dos dados em exercerem os seus direitos.

Aplicação de metodologia DPIA

Desenho dos Fluxos de Informação

Como primeiro passo metodológico, será necessário desenhar os fluxos de dados pessoais previstos para cumprimento da finalidade de tratamento subjacente, desde a recolha até ao final do processo de tratamento dos dados, passando por todos os seus intervenientes.

Identificação de Riscos

Subsequentemente, o processo de avaliação de risco deve ser detalhado, rigoroso e alinhado com os requisitos do RGPD e de outros requisitos legais regulatórios aplicáveis, nomeadamente, da LPD, sendo que os riscos podem estar associados aos titulares dos dados, clientes, fornecedores ou Colaboradores (ex. pessoais, morais, intrusão) ou o BCGA (ex. reputação, financeiros, legais/*compliance*). A categorização e classificação dos riscos resulta de uma avaliação qualitativa que considera a sua probabilidade de ocorrência e severidade do seu impacto.

Identificação de Medidas de Mitigação

Caso os riscos identificados pelo Órgão de Estrutura responsável pelo produto, processo ou tecnologia não sejam compatíveis com as exigências do RGPD e de outros requisitos legais regulatórios aplicáveis, nomeadamente, da LPD, o BCGA deve elaborar um plano de acção para a sua mitigação. Este plano pode contemplar iniciativas de controlo, transferência (ex. seguro) ou eliminação dos riscos (ex. eliminação de um fluxo de informação secundário ao propósito principal do projecto de desenho/revisão), devendo ser definidas acções tendo em consideração uma análise custo-benefício e o impacto no propósito do tratamento.

Plano de Implementação das Medidas

Após conclusão do processo de avaliação, os Órgãos de Estrutura responsáveis devem detalhar o plano de acção resultante, integrando as soluções propostas para mitigação do risco no contexto das suas actividades no âmbito do projecto de desenho/revisão do produto, processo, tecnologia/sistema. Este plano deve ser implementado o mais cedo possível, decorrendo ao longo da concepção/implementação das actividades de processamento em causa.

Elaboração de Relatório

Todos os envolvidos no tratamento de dados devem ser notificados das conclusões do DPIA e das acções resultantes, através do relatório final produzido após o *assessment (vide* estrutura de relatório no Anexo III). O registo do processo serve ainda como evidência futura no caso de reavaliações ou necessidades de avaliação sobre tratamentos de dados equiparáveis ou similares.

Consulta prévia a Autoridades de Controlo (APD)

Caso se conclua que, mesmo após medidas de mitigação, há um risco elevado do produto/processo/tecnologia ou sistema não cumprir as exigências regulamentares (ex. no que diz respeito ao exercício dos direitos dos titulares dos dados), o responsável pelo tratamento deve comunicar ao *Data Protection Officer* que assegurará a notificação, caso necessário, à APD, por forma a obter desta uma posição/aconselhamento sobre a adequação das medidas de mitigação de risco propostas e a viabilidade de implementação do projecto tendo em conta o risco residual associado. Este procedimento não é obrigatório e resulta de uma análise casuística do impacto previsto no projecto de desenho/revisão em questão.

Quando for aplicável a LPD e subsidiariamente o RGPD e caso se conclua que, mesmo após medidas de mitigação, há um risco elevado do produto/processo/tecnologia ou sistema não cumprir as exigências regulamentares (ex. no que diz respeito ao exercício dos direitos dos titulares dos dados), o responsável pelo tratamento, com conhecimento do Órgão de Administração, deve comunicar ao *DPO* que, com a colaboração do *Data Protection Officer* corporativo, assegurará a notificação, caso necessário, à APD ou à CNPD, por forma a obter desta uma posição/aconselhamento sobre a adequação das medidas de mitigação de risco propostas e a viabilidade de implementação do projecto tendo em conta o risco residual associado. Este procedimento não é obrigatório e resulta de uma análise casuística do impacto previsto no projecto de desenho/revisão em questão.

Reavaliação do risco

Após a condução do processo DPIA e implementação de medidas de mitigação dos riscos, será importante definir responsáveis pela sua monitorização e reavaliação. Este acompanhamento deve ser periódico ou sempre que se verifique uma alteração ao produto/processo/tecnologia ou sistema em causa ou uma alteração do quadro legislativo, sendo a periodicidade do acompanhamento definida consoante a severidade que lhe é associada, não podendo nunca exceder os 3 anos.

4.1.3. Violação de dados pessoais[4]

O BCGA, na qualidade de responsável pelo tratamento de dados pessoais, está obrigada, em caso de violação de dados pessoais, a notificar a APD desse facto, sem demora injustificada e, sempre que possível, até 72 horas após conhecimento da violação. O *Data Protection Officer* dá imediato conhecimento ao *Data Protection Officer* corporativo da notificação da violação de dados efectuada perante a APD, disponibilizando a documentação respectiva e prestando toda a informação.

A notificação à APD não é obrigatória nos casos em que a violação de dados pessoais não seja susceptível de resultar num risco para os direitos e liberdades das pessoas singulares.

No caso de não ser possível fornecer, na notificação à APD, todas as informações ao mesmo tempo, podem as mesmas ser fornecidas faseadamente, sem demora injustificada.

O responsável pelo tratamento documenta todas as violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respectivos efeitos e a medida de reparação adoptada, devendo permitir à APD verificar a respectiva conformidade com as disposições legais aplicáveis.

Sem prejuízo das orientações a emitir nomeadamente pela APD e outras autoridades de controlo sobre protecção de dados[5], bem como das soluções a consagrar em normativo interno específico que regule esta matéria, a notificação relativa à violação de dados pessoais deve conter, pelo menos, os seguintes elementos (*triggers* – Anexo IV):

a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afectados em causa;

b) Comunicar o nome e os contactos do *Data Protection Officer* ou de outro ponto de contacto onde possam ser obtidas mais informações, além do responsável pelo tratamento;

c) Descrever as consequências prováveis da violação de dados pessoais;

d) Descrever as medidas adoptadas 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.

Quando a violação dos dados pessoais for susceptível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados, o responsável pelo tratamento comunica-lhes, sem demora injustificada, a violação de dados pessoais.

Conforme disposto na Política de Protecção de Dados Pessoais, os Colaboradores e os prestadores de serviços (v.g. subcontratantes) estão obrigados a reportar internamente, logo que dela tenham conhecimento, qualquer situação que configure uma violação de dados pessoais.

Os subcontratantes estão obrigados a cooperar activamente com o BCGA, reportando imediata e cumulativamente ao Órgão de Estrutura que gere o contrato e ao *Data Protection Officer*, as situações de violação de dados pessoais em termos de o BCGA poder cumprir, no prazo legal de 72 horas, o dever de notificação à APD[6]. Os subcontratantes estão ainda obrigados, nos termos do contrato respectivo, a prestar ao BCGA a colaboração necessária para reparar a situação.

Para este efeito, os subcontratantes articulam-se com o respectivo gestor da relação contratual, cabendo a este assegurar no BCGA os mecanismos e procedimentos adoptados para notificação à APD e comunicação aos titulares de dados, quando for o caso.

Em ordem a garantir que todas as situações de violação de dados pessoais são reportadas, estabelece-se o seguinte procedimento interno a adoptar pelos Órgãos de Estrutura envolvidos:

a) O Colaborador que detecte ou tenha conhecimento de situação que possa configurar violação de dados, deve reportar ao Pivot de Protecção de Dados do seu OE, que irá registar de imediato a mesma, em sede de Catálogo de Serviços;

b) O Pivot de Protecção de Dados em articulação com o Director do OE (ex. DAI, DOQ, DPO, DSI e GPS) analisam a situação reportada;

c) Caso concluam pela verificação de uma violação de dados pessoais, comunicam ao *Data Protection Officer* e, em simultâneo, procede ao registo da situação.

d) A comunicação aos titulares de dados afectados deve observar o Manual de comunicação do BCGA e ser feita em linguagem clara e simples, identificando a natureza da violação de dados, o

---

[4] Violação de dados pessoais é uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento [cf., neste sentido, o art. 4.º, 12), do RGPD]. Aplicável ao BCGA por via da CGD.

[5] Tais como o Comité Europeu para a protecção de Dados e a Comissão Nacional de Protecção de Dados, de Portugal.

[6] Cf., em especial, os artigos 33.º e 34.º aplicáveis "*ex vi*" do artigo 28.º, n.º 3, al. f), do RGPD. Aplicável ao BCGA por via da CGD.

nome e os contactos do *Data Protection Officer*, elencando as possíveis consequências da violação e as medidas adoptadas para reparar os impactos negativos;

e) O *Data Protection Officer* comunica aos titulares dos dados e documenta o teor da comunicação.

Todo o processo relativo à violação de dados pessoais deve ser documentado a fim de poder ser evidenciado à APD, caso seja necessário.

4.1.4. Resposta aos direitos dos titulares

O BCGA, na qualidade de responsáveis pelo tratamento de dados pessoais, estão obrigadas a assegurar o exercício dos direitos dos titulares, descritos em detalhe no normativo que consubstancia a Política de Protecção de Dados Pessoais e a Política de Privacidade e de Protecção de dados Pessoais, a saber:

a) Direito de acesso – prestação de informação sobre os dados pessoais dos titulares a cujo tratamento o BCGA procede no âmbito da sua actividade;

b) Direito de rectificação – correcção, actualização ou inclusão de informação (que possa estar em falta) relativa aos titulares dos dados;

c) Direito ao apagamento dos dados ("direito a ser esquecido") – apagamento dos dados pessoais, verificados os requisitos legais para o efeito (inexistência de contratos activos, dados desnecessários para a finalidade que motivou a sua recolha e /ou tratamento, ultrapassado o prazo legal de conservação dos dados a que o BCGA está obrigado);

d) Direito à limitação do tratamento – suspensão/cessação (temporária) do tratamento de dados, observados os requisitos legais aplicáveis;

e) Direito de oposição – revogação de consentimento para tratamento(s) de dados efectuado(s) com base nesse fundamento.

O titular dos dados deve formalizar o pedido para o exercício dos direitos por escrito, sendo que, uma vez garantida a identificação do titular, o BCGA responde ao pedido sem demora injustificada e no prazo de um mês após a recepção do pedido. Este prazo pode ser prorrogado até 2 meses, mediante justificação a prestar até um mês após a apresentação do pedido.

Ao titular dos dados é fornecido um comprovativo do pedido efectuado (cópia simples do formulário preenchido, datado e assinado pelo titular dos dados e pelo Colaborador receptor).

A satisfação dos direitos é efectuada gratuitamente, excepto se os pedidos apresentados pelo titular dos dados forem manifestamente infundados ou excessivos, cabendo essa prova ao BCGA.

Os procedimentos e meios disponíveis para o exercício de direitos pelos titulares dos dados são divulgados pelo BCGA:

a) Através da Política de Privacidade e de Protecção de Dados Pessoais, divulgada em www.caixaangola.ao. Sem prejuízo dos procedimentos detalhados a estipular em normativo interno específico que regule esta matéria, a resposta aos direitos do titular, é assegurada conforme consta *infra*:

Resposta a Clientes BCGA

a) O Cliente (titular dos dados) formaliza o pedido de exercício de direitos através da Rede Comercial (em impresso próprio);

b) O Colaborador garante:

   i. a correcta instrução do pedido de exercício de direitos (*v.g.* entrega de comprovativos, no caso de pedido de rectificação de elementos que o exijam);

   ii. quando aplicável, a validação da identidade do titular;

   iii. a digitalização do pedido de exercício de direitos e seu arquivo na pasta própria;

c) O tratamento do pedido é efectuado nos seguintes termos:

   i. direito de acesso – o receptor trata o pedido mediante acesso à plataforma de balcão, imprimindo ou gravando ficheiro com a informação correspondente à constante da Ficha de Elementos Informativos e/ou à informação particular solicitada pelo Cliente, procedendo à sua entrega nos moldes pretendidos;

   ii. direito de rectificação – o receptor do pedido actualiza na transacção respectiva a informação fornecida pelo cliente, devidamente comprovada quando for o caso;

   iii. direito de oposição – o receptor do pedido regista na plataforma de balcão a revogação do consentimento prestado, nos termos solicitados pelo titular dos dados;

iv. direito ao apagamento dos dados (“direito a ser esquecido”) e direito à limitação do tratamento – o receptor encaminha pedido através de AGILE para o CO, que avalia se o Cliente reúne requisitos para o efeito pretendido, procede ao registo respectivo no sistema de informação, quando aplicável, e responde ao Cliente em conformidade;

d) Quando o pedido suscite dúvidas de natureza jurídica à Rede Comercial, deverá ser solicitada a apreciação do GAJ.

Resposta a Colaboradores e a candidatos a Colaboradores do BCGA

a) O Candidato solicita exercício dos direitos através de email dirigido a drh@caixaangola.ao,os Colaboradores através do Caixa pessoal, por carta ou email dirigido a drh@caixaangola.ao; os ex-Colaboradores, por carta ou email dirigido a drh@caixaangola.ao; podendo a DRH solicitar apoio sempre que necessário através data.protection@caixaangola.ao;

b) A Direcção de Recursos Humanos (DRH) valida a identidade do titular dos dados;

c) A Direcção de Recursos Humanos (DRH) assegura a resposta ao pedido do titular dos dados com conhecimento da Data *Protection Officer.*

4.1.5. Emissão de pareceres

No âmbito da protecção de dados pessoais, poderão ser colocadas dúvidas ao Data *Protection Officer*, através da *mailbox* data.protection@caixaangola.ao .

Sem prejuízo dos pedidos de parecer e/ou aconselhamento dirigidos ao Data *Protection Officer* poderão estas suscitar a intervenção, sobre questões de protecção de dados, do Data *Protection Officer* corporativo, para que este se pronuncie. Para o efeito, deverá ser utilizada a *mailbox* data.protection.officer@cgd.pt.

4.1.6. Acompanhamento das Entidades CGD

O Grupo CGD desenvolve o seu negócio a nível nacional e internacional, através de Filiais e Sucursais, devendo o BCGA assegurar a conformidade da sua actividade com a legislação e regulamentação aplicáveis nas respectivas jurisdições.

O acompanhamento do BCGA assenta, além dos processos específicos de gestão de protecção de dados abordados nos pontos anteriores, num conjunto de processos e procedimentos de natureza transversal.

Pretende-se uma cooperação estreita e um diálogo fluído entre a CGD e o BCGA, com vista a assegurar o alinhamento com a estratégia da CGD e a difundir uma cultura organizacional de protecção de dados e a partilha de experiências.

Compete ao *Data Protection Officer* corporativo acompanhar e monitorizar à distância as práticas e procedimentos implementados e executados pelo BCGA no âmbito da conformidade sobre protecção de dados, colaborando no levantamento de necessidades e na implementação de projectos, em cooperação com os respectivos Órgãos de Administração ou de gestão de topo (cf. ponto 1.2), os *Data Protection Officer* local (cf. ponto 1.4).

O *Data Protection Officer* define e analisa os reportes efectuados pelo BCGA em matéria de protecção de dados para acompanhamento da respectiva actividade (cf. ponto V) e elabora um relatório de ponto de situação da actividade do BCGA, tendo por base os relatórios imediatos, semestrais e outra informação recebida, com a finalidade de fornecer ao Órgão de Administração informação sistematizada das principais ocorrências registadas no semestre.

5. MONITORIZAÇÃO E REPORTE

5.1 No âmbito das actividades de acompanhamento e monitorização devem ser assegurados os reportes tempestivos a seguir indicados.

Relatório de Acompanhamento da Protecção de Dados do *Data Protection Officer* ao **Comité de Risco Operacional e Controlo Interno (ROCI)**

O *Data Protection Officer* apresenta, até final do 1.º trimestre do ano seguinte, o relatório anual de actividades em matéria de protecção de dados. O relatório versa, entre outros aspectos, a avaliação da eficácia da protecção de dados a nível central e local e procede à identificação dos principais riscos para o BCGA a CGD (enquanto responsável pelo tratamento de dados) e os titulares dos dados, bem como das questões concretas para as quais se considera necessário o enforcement da gestão de topo.

5.2. Reporte de eventos de violação de dados pessoais

No caso de violação de dados (cf. ponto 4.1.3.), o Órgão de Estrutura onde ocorreu a situação de violação de dados elabora reporte para apresentação ao *Data Protection Officer*, por outro lado, à elaboração do reporte também ao DPO Corporativo, pelo DPO local, por cada ocorrência, que inclua a descrição do evento e volumetria associada, a apresentação das medidas correctivas e das medidas preventivas a adoptar, bem como a notificação (ou não) à APD e, caso aplicável, a comunicação aos titulares de dados pessoais afectados.

5.3. Reporte do BCGA sobre protecção de dados ao *Data Protection Officer* corporativo

O BCGA elabora um relatório semestral sobre protecção de dados para apresentação ao *Data Protection Officer* corporativo que verse sobre o estado de conformidade com RGPD e a LPD, bem como com a Política de Protecção de Dados Pessoais corporativa e demais normativos internos conexos. O relatório deve também incluir as acções desenvolvidas para assegurar a conformidade com RGPD e a LPD, as principais actividades planeadas e desenvolvidas e a identificação de necessidades concretas de apoio central no âmbito da protecção de dados.

6. DISPOSIÇÕES FINAIS

O BCGA deve adoptar metodologias de operacionalização da gestão de protecção de dados que respeitem o disposto na presente Ordem de Serviço.

ANEXO I – MATRIZ DE RESPONSABILIDADE (RACI)

	Principais Funções	Adm CGD	Adm BCGA	DPO Corp	DPO	OE Resp Trat	DCO	OE Risco[7]	OE [8]	Colab. BCGA
Governance	Gestão global do Modelo de Governo: • Planeamento da Gestão da Protecção de Dados • Manutenção e actualização da Política de Protecção de Dados e do Modelo de Governo • Monitorização e Reporte • Articulação entre os Órgãos Sociais e restantes intervenientes	I	A	C	R					
Registo: Inventário de Tratamento	• Caraterização dos tratamentos de dados efectuados				I/C	R				
	• Avaliação da fundamentação legal e eventuais vulnerabilidades				I/C	R				
	• Incorporação de optimizações face às vulnerabilidades identificadas				I	R				
	• Actualização do inventário			I	C	R				
Metodologia e Processo DPIA	• Avaliação da necessidade de DPIA					R				
	• Realização do DPIA				S	R				
	• Implementação de medidas de mitigação					R				
	• Consulta prévia à CNPD			S	S	R				
	• Reavaliação do Risco					R				
Gestão da Violação de Dados Pessoais	• Reporte e registo de violação de dados pessoais						I		I	R
	• Análise da situação e implementação medidas reparação				I	S			R	
	• Decisão de notificação à CNPD e comunicação aos titulares dos dados		C	I	S	R				
	• Notificação à CNPD			I	I	R				
	• Comunicação aos Titulares Dados				S	R				
	• Registo em repositório das situações comunicadas								R	
Resposta aos Direitos Titulares	• Receção de pedido de exercício de direitos								R	
	• Análise do pedido				C				R	
	• Resposta ao titular dos dados								R	
Consulta DPO	• Solicitação de Parecer					R				
	• Emissão de Parecer			I	R					

[7] Responsabilidades e actividades a definir pelo BCGA.
[8] Responsabilidades e actividades a definir pelo BCGA.

ANEXO II – Template de Avaliação da Necessidade de uma Avaliação de Impacto Sobre Protecção de Dados (DPIA)

Finalidade do tratamento	
Base de licitude para o tratamento	
Categorias de dados tratados	
Dimensão de titulares afetados (n.º aprox.)	
Sistemas tecnológicos utilizados	

Questões de enquadramento	**Sim**	**Não**
Será necessária a recolha de dados pessoais que ainda não sejam tratados pela CGD?		
Será necessária a disponibilização de dados pessoais a pessoas/entidades que ainda não tenham acesso aos mesmos?		
Será necessária a utilização de dados pessoais que ainda não eram recolhidos para a finalidade indicada?		
Será necessária a utilização de tecnologia e/ou meios contacto que possam ser considerados intrusivos pelos titulares?		

***Checklist* de avaliação da necessidade** *(indique se as seguintes atividades estão implicadas no produto/processo/sistema)*	**Sim**	**Não**
Tratamento para fins de avaliação ou *scoring* de pessoas singulares		
Tratamento como base para tomada de decisões automáticas que produzem efeitos significativos no titular (ex. como *profiling)*		
Tratamento de informação em larga escala (i.e. elevado volume de dados, número de titulares afetados, longa duração ou abrangência geográfica)		
Monitorização sistemática de pessoas singulares (ex. em áreas públicas)		
Tratamento de dados sensíveis (ex. dados biométricos, médicos, legais – art. 9.º)		
Tratamento de dados relativos a pessoas singulares em situações de vulnerabilidade (como colaboradores, indivíduos incapacitados, menores)		
Utilização de dados que foram correspondidos ou combinados, provenientes de duas ou mais fontes e/ou operações de tratamento de dados		
Recurso a novas soluções tecnológicas que ainda não se encontrem em utilização na organização		
Transferência de dados pessoais para fora da União Europeia		
Dificuldade dos titulares dos dados em exercerem os seus direitos		

ANEXO III – ESTRUTURA DE RELATÓRIO DPIA

1. **Introdução**

   a) Informação geral sobre o processo/produto/sistema em análise

   b) Referências a políticas e leis aplicáveis

   c) Identificação do responsável pelo tratamento e condutor do DPIA

2. **Avaliação da necessidade de um DPIA**

   a) Descrição do motivo que desencadeou o DPIA

   b) Identificação do responsável pelo alerta da necessidade

   c) Conclusões do preenchimento do formulário de avaliação da necessidade (Anexo IV)

3. **Âmbito do DPIA**

   a) **Descrição das actividades de tratamento**

   i. Natureza, âmbito, contexto e finalidades do tratamento

   ii. Descrição funcional das operações de tratamento

   iii. Visão geral dos dados utilizados no contexto das actividades de tratamento

   iv. Identificação de transferências de dados (produto do desenho dos fluxos)

   v. Descrição, de alto nível, dos sistemas envolvidos (*hardware, software*, redes, etc.)

   vi. Descrição das medidas de segurança aplicadas

   b) ***Stakeholders***

   vii. Descrição do envolvimento dos *stakeholders*

   viii. Opiniões dos titulares dos dados, ou dos seus representantes, quando aplicável

   ix. Parecer do *Data Protection Officer*

   x. Parecer de outros Órgãos de Estrutura relevantes

   c) **Descrição dos critérios de risco**

   Identificação dos riscos mais relevantes (ex. acesso/alterações não autorizados, perda, violação de direitos dos titulares, ausência de bases legais, etc.)

   d) **Objectos de risco**

   Identificação das fontes do risco (ex. *hardware/software*/pessoas/documentos)

   e) Avaliação de risco

   i. Os critérios de risco devem ter em consideração a perspectiva do titular dos dados

   ii. Avaliação do impacto para cada risco identificado pelo Órgão de Estrutura de acordo com os graus de risco:

   - Nulo / muito reduzido: sem efeito no titular dos dados;
   - Reduzido: inconveniências não significativas para o titular dos dados (ex. perda de tempo, perda de serviços, custos extra)
   - Elevado: consequências significativas que os titulares dos dados ainda consigam ultrapassar (ex. fraude, roubo de identidade, entrada em listas negras)
   - Muito elevado: consequências significativas que poderão ser irreversíveis, ou que o titular dos dados não consiga ultrapassar (ex. perda de emprego, ameaças à saúde)

   iii. Quantificação da probabilidade para cada evento identificado na mesma escala (nulo / muito reduzido, reduzido, elevado, muito elevado)

   iv. Combinação entre o impacto e a probabilidade de cada risco (ex. média quadrática)

   v. Descrição dos critérios definidos para aceitação do risco.

4. **Plano de mitigação de riscos**
    a) Lista de medidas identificadas para mitigar os riscos
    b) Detalhe das medidas definidas (intervenientes, metodologia, impacto esperado)
    c) Descrição do risco residual (i.e. após aplicação das medidas)
    d) Planeamento da implementação das medidas (calendarização e responsabilização)
    e) Inventariação das necessidades para cumprimento do plano (recursos humanos ou materiais)
5. **Decisões**
    a) Documentação da aprovação/rejeição das medidas
    b) Pareceres finais do *Data Protection Officer* e Órgãos de Estrutura envolvido

ANEXO IV – *TRIGGERS* - VIOLAÇÃO DE DADOS

Incidentes de segurança física	Incidentes de segurança lógica/informática
Furto ou extravio de equipamento electrónico (portátil, dispositivos amovíveis)	*Malware* (*ransomwares*)
Furto ou extravio de documentos em suporte de papel	*Phishing* (apropriarem-se das credenciais)
Perda de chaves electrónicas	*Hacking*
Incêndio nos servidores de dados do *Data Center*	*Ewaste* (dados pessoais ainda presentes em dispositivo obsoleto)
Extravio ou abertura ilícita de correio	Divulgação não intencional (envio de *email* para destinatário errado, caso de campanhas em que os clientes vão em Bcc, etc.)
Destruição incorrecta de papel com informação sensível	Acção deliberada ou por inércia de um Colaborador/ prestador
Divulgação verbal não autorizada de dados pessoais	Alteração de dados pessoais sem autorização
Acesso não autorizado de terceiros	Indisponibilidade de dados pessoais