# Princípios da protecção de dados pessoais em locais de trabalho

## —— Instruções para fiscalização das actividades dos empregados pelos empregadores

Com o objectivo de implementar com eficácia a Lei n.° 8/2005 (doravante designada por Lei da Protecção de Dados Pessoais), foram elaboradas estas instruções, para garantir a protecção de dados pessoais, e instruir aos empregadores, depois de terem reflectido em pormenor e meticulosamente, estabeleçam a respectiva política de fiscalização dos empregados, evitando a violação das leis por parte dos empregadores.

Estas instruções só são aplicáveis à fiscalização das actividades dos empregados pelos empregadores dos Serviços Públicos e entidades privadas (doravante designada por entidade).

## 1. O acto de fiscalização é um acto de tratamento de dados pessoais

A fiscalização de actividades dos empregados feita pelos empregadores normalmente pode envolver fiscalização de chamadas telefónicas, de correio electrónico, de visualização de *internet*, por videogravação.

A fiscalização de chamadas telefónicas significa, fiscalizar e registar os números de telefone, conversas ou recados recebidos ou emitidos pelos empregados através dos equipamentos de telecomunicações fornecidos pelos empregadores, gravando, assim, os sons das pessoas em causa.

A fiscalização de correio electrónico significa, fiscalizar e registar o correio electrónico recebido e enviado pelos empregados através dos equipamentos

fornecidos pelos empregadores, recolhendo, assim, os endereços e conteúdo de correio electrónico recebidos e enviados pelos empregados.

A fiscalização da utilização da *internet* significa, fiscalizar e registar as actividades de visualização da *internet* pelos empregados através dos equipamentos fornecidos pelos empregadores, recolhendo, assim, os registos de visualização do titular de conta e as informações transmitidas e recebidas.

A fiscalização por videogravação significa, instalar câmaras de vídeo ou circuito fechado de televisão, entre outros equipamentos no local de serviço, para efeitos de registo dos empregados e das pessoas que se movimentam nessa área, recolhendo, assim, as imagens dos empregados e de outras pessoas.

O acto de fiscalização das actividades dos empregados pelos empregadores envolve a recolha e tratamento de dados pessoais.

Nos termos do artigo 4.° da lei supramencionada, "Dados Pessoais" indicam: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»), sendo considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social. Tais como: nome, sexo, data de nascimento, idade, estado civil, morada, telefone, fax, correio electrónico, local de trabalho, funções, rendimento, número do cartão de eleitor, conta bancária, fotografia, gravação de imagem e som, entre outros.

"O tratamento de dados pessoais" inclui: qualquer ou uma série de operações que diga respeito a dados pessoais, independentemente da operação utilizar meios automatizados ou não, tais como: recolha de dados, registo, disposição, conservação, recomposição ou alteração, recuperação, consulta, utilização ou comunicação com

outras pessoas mediante transmissão, divulgação ou outras formas de comparação ou interligação, incluindo também o bloqueio, apagamento e destruição de dados.

Nos termos do artigo 3.° da Lei da Protecção de Dados Pessoais, a referida lei "aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados". Por isso, os actos de fiscalização das actividades indicados acima são regulamentados pela Lei da Protecção de Dados Pessoais.

## 2. Avaliação prévia das actividades de fiscalização feita pelos empregadores

Em virtude das actividades de fiscalização de chamadas telefónicas, de correio electrónico, de visualização da *internet* e por videogravação envolverem a recolha de dados pessoais dos empregados, os empregadores antes de procederem à fiscalização acima mencionada das actividades dos empregados, devem reflectir meticulosamente, nomeadamente, sobre as seguintes questões:

1. Quais são os objectivos da recolha, estes são lícitos ou não?
2. As medidas de fiscalização são verdadeiramente necessárias para alcançar os objectivos? Existem ou não outros métodos que tratando menos os dados pessoais possam substituí-las?
3. As medidas, a área e o período de fiscalização são adequados?
4. Os dados a recolher são verdadeiramente necessários para alcançar os objectivos?
5. A fiscalização contribui para garantir os interesses dos empregadores, empregados e destinatários dos serviços?

6. Caso os dados recolhidos sejam tratados inadequadamente, que danos poderão daí ocorrer?
7. Como estabelecer um código de conduta para proteger os dados pessoais e como elaborar a declaração para a recolha de dados pessoais?

## 3. Princípios a seguir para proceder à fiscalização dos empregados

Sendo as actividades de fiscalização actos de recolha de dados pessoais, os actos de fiscalização dos empregados pelos empregadores devem cumprir as normas da Lei da Protecção de Dados Pessoais, o tratamento de dados pessoais deve processar-se de forma transparente e lícita, no respeito pela reserva da vida privada, bem como no cumprimento do estipulado sobre os direitos fundamentais, liberdades e garantias estabelecido pela lei e, devendo cumprir também o princípio da boa fé (*vide* o artigo 2.° e a alínea 1) do n.° 1 do artigo 5.° da Lei da Protecção de Dados Pessoais). A violação dos princípios estipulados neste ponto 3 pode cometer a infracção administrativa ou criminal, e enventualmente o empregador em causa indemnizará também o(s) ofendido(s). (*vide* o artigo 14.° e o artigo 30.° a 44º da Lei da Protecção de Dados Pessoais)

### (1) Princípio da legalidade

O princípio da legalidade do tratamento de dados pessoais inclui três aspectos: a legalidade do objectivo, das formas e dos âmbitos.

1. Legalidade do objectivo

Dum modo geral, o objectivo pelo qual os empregadores efectuam a recolha de dados pessoais e fiscalizam o comportamento dos empregados em locais de trabalho baseia-se nas necessidades de funcionamento da entidade e, para garantir os interesses

dos empregadores. Sendo um empregador fiscalizar o trabalho dos empregados dentro da área de exploração ou dentro da área da sua competência e por razões de funcionamento, negócio e necessidade geral, o objectivo é lícito.

No decorrer da fiscalização, os principais factores que os empregadores devem ter em conta são:

---- São medidas necessárias para garantir a segurança dos empregados?

---- Corre-se o risco de perda e prejuízo de patrimónios importantes?

---- Há grande necessidade de segurança devido à natureza da entidade?

---- Corre-se o risco dos empregados poderem revelar confidências da entidade para outras instituições ou para outras pessoas?

---- Existem empregados que tratam de actividades privadas durante o tempo de trabalho e que afectam a eficácia do trabalho?

---- O sistema da entidade será afectado por motivo da utilização inadequada do equipamento de informática?

---- Os empregados prestam bons serviços aos destinatários do serviço? Quando existem queixas dos destinatários, como garantir os interesses das três partes, da entidade, empregados e destinatários?

---- Como reduzir os efeitos negativos que afectam as boas relações de cooperação e confiança mútua entre empregador e empregados daí resultantes.

2. Legalidade das formas

Deve-se efectuar a fiscalização de forma lícita, os métodos adoptados devem ser necessários para alcançar o objectivo. As formas de fiscalização devem ser reveladas ao público, não devendo ser efectuadas com truques e em segredo. O prazo de conservação dos dados obtidos deve estar dentro do prazo adequado e necessário para alcançar o objectivo. Sugere-se o prazo de conservação de três meses, não

ultrapassando seis meses para as situações especiais.

3. Legalidade dos âmbitos

Os âmbitos de fiscalização devem ser limitadas às actividades respeitantes ao trabalho dos empregados, não devendo incluir conteúdos relacionados com a vida privada dos empregados. Caso contrário, a privacidade destes empregados será violada, infringindo assim o estipulado no artigo 30.° da Lei Básica da Região Administrativa Especial de Macau ("... Aos residentes de Macau são reconhecidos ... o direito à reserva da intimidade da vida privada e familiar.") como *por exemplo, as câmaras de vídeo ou circuitos fechados de televisão não devem ser instalados em salas de descanso ou vestiários dos empregados, não devendo fiscalizar os conteúdos do correio electrónico enviados pelos empregados para os seus familiares fora do horário de trabalho, etc.*

**(2) Princípios moderados**

Os princípios moderados aqui referidos incluem principalmente os princípios de interferência adequada e em grau mínimo.

(1) Caso a substituição por outras medidas possa alcançar o objectivo da recolha de dados pessoais, ou seja, a recolha de dados pessoais é prescindível, não se deve efectuar a recolha. Tal como, para evitar a invasão de vírus de informática, os empregadores podem instalar a Parede Contra Fogo ou *software* de filtragem no sistema informático, bem como podem dar instruções explícitas aos empregados, explicando os tipos de páginas electrónicas que não podem ser visualizadas, não devendo recolher os dados visualizados pelos empregados na *internet*.

(2) A fiscalização é feita apenas a propósito de actividades de alto risco e é implementada em áreas de alto risco, limitando-se apenas a assegurar os

interesses legais dos empregadores e evitar riscos latentes. E não se deve recolher os dados dos empregados que não dominam os dados confidenciais da entidade, ou os dados pessoais dos empregados que não constituam riscos; assim como em relação ao correio electrónico assinalado como correio privado, o mesmo não deve ser fiscalizado. Não se procede à fiscalização por videogravação em áreas sem alto risco. Tais como: instalar apenas câmaras de gravação ou circuitos fechados de televisão em lugares onde estejam armazenados dados, arquivos, materiais e sistemas confidenciais ou sensíveis.

(3) Diminuir tanto quanto possível o período de fiscalização, não fiscalizar as actividades dos empregados fora do horário de trabalho.

(4) O grau de fiscalização deve ser equiparado ao grau necessário para atingir o objectivo, de modo a diminuir o mais possível a recolha e tratamento dos dados pessoais. Como *por exemplo: efectua-se apenas o registo dos endereços de correio electrónico recebidos ou enviados, dos números de telefone emitidos ou recebidos pelos empregados, mas, no caso de ser desnecessário, não se procede à inspecção dos respectivos conteúdos*. Só se procede à re-examinação dos conteúdos de telefonemas, correio electrónico, e videogravação caso haja necessidade, *por exemplo: no caso de recepção de queixa do destinatário de serviços contra o empregado, é preciso re-examinar os conteúdos da gravação telefónica ou do correio electrónico nos trabalhos de averiguação. Durante a re-examinação dos respectivos registos, excepto averiguação sobre infracção disciplinar, infracção administrativa ou investigação criminal, é conveniente ter a presença do titular.*

**(3) Princípio da garantia dos interesses do titular dos dados**

O acto de fiscalização dos empregados nos locais de trabalho deve ser publicado, (de forma transparente), por forma a que seja assegurada a execução dos direitos do titular dos dados. Nos termos da Lei da Protecção de Dados Pessoais, os titulares dos dados têm direito de informação, direito de acesso, e direito de oposição (*vide* os artigos 10.° a 12.° da respectiva lei).

1. Direito de informação

Quando recolher dados pessoais, a entidade deve prestar ao titular dos dados as seguintes informações, se tiver o documento de recolha de dados pessoais deve constá-las do documento:

(1) Identidade do responsável pelo tratamento e, se for caso disso, do seu representante;

(2) Objectivos do tratamento:

Tais como, garantia de segurança do sigilo económico da entidade, garantia da qualidade de serviços, garantia de segurança dos materiais com valores elevados, etc.

(3) Destinatários dos dados ou tipos de destinatários:

Significa, durante a fiscalização, se os dados recolhidos serão ou não, entregues a outras entidades para efeitos de conhecimento ou tratamento. Caso os dados pessoais sejam tratados pelo subcontratante, deve-se também comunicar ao empregado.

Normalmente, estes dados são registados no sistema da respectiva entidade, não necessitando de ser tratados novamente por terceiros. No entanto, o empregador deve indicar os responsáveis pela fiscalização e tratamento dos dados envolvidos, devendo também esclarecer que os respectivos dados serão entregues

aos Serviços competentes, autoridades de investigação criminal e judiciárias para serem re-examinados por motivos de infracção disciplinar ou infracção jurídica.

(4) Resposta obrigatória ou facultativa do titular, e os resultados provenientes do facto de não responder.

É aplicável às situações que envolvam perguntas, respostas e investigação durante a recolha de dados.

(5) Tendo em consideração as situações especiais da recolha de dados, com vista a assegurar que os dados do titular sejam tratados com veracidade, em caso de necessidade, devem ser criadas as condições para que o titular dos dados possa exercer o direito de acesso e de rectificação (*vide* o Direito de acesso).

2. Direito de acesso

Um empregado, sendo titular dos dados tem direito de solicitar o acesso aos seus próprios dados livremente e sem restrições, devendo o empregador proporcionar-lhe os respectivos dados dentro de um prazo racional. O empregado tem direito de acesso ao seguinte:

(1) A confirmação de serem ou não tratados dados que lhe digam respeito, bem como informação sobre as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados;

(2) A comunicação, sob forma inteligível, dos seus dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem desses dados;

(3) O conhecimento das razões subjacentes ao tratamento automatizado dos dados que lhe digam respeito;

(4) A rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na Lei da Protecção de Dados Pessoais, nomeadamente devido ao carácter incompleto ou inexacto desses dados;

(5) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos do ponto (4), salvo se tal for comprovadamente impossível ou implicar um esforço manifestamente desproporcionado, devendo os terceiros proceder igualmente à rectificação, apagamento, destruição ou bloqueio dos dados.

3. Direito de oposição

No pressuposto de não haver incompatibilidade legal, o titular dos dados tem o direito de se opor em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento. Devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados.

## 4. Assuntos a observar na elaboração da Declaração de recolha de dados pessoais para fiscalizar as actividades dos empregados

Antes de proceder à fiscalização dos empregados, os empregadores devem elaborar para o efeito, uma declaração explícita e clara sobre a recolha de dados pessoais, devendo nesta declaração indicar o seguinte:

1. O objectivo da fiscalização dos empregados. *Por exemplo, a gravação telefónica destina-se apenas para assegurar a qualidade de serviços, ou também para a avaliação do desempenho dos empregados; o objectivo da videogravação destina-se por razões de segurança, ou destina-se também para a classificação de assiduidade;*
2. Tipos de dados pessoais a recolher por motivo da fiscalização;
3. Finalidade da utilização de dados pessoais recolhidos por motivo da fiscalização. A finalidade da utilização de dados pessoais não pode

desviar-se do objectivo da fiscalização;

4. Critérios da utilização de dados pessoais recolhidos por motivo da fiscalização. *Por exemplo, indicar na declaração sobre a fiscalização de correio electrónico que, na fiscalização dos conteúdos de correio electrónico privado, apenas se efectua o registo de utilização, caso necessário, deve-se especificar as situações em que se procede à fiscalização dos conteúdos do correio electrónico; quanto aos dados da videogravação, são observados periodicamente ou só quando surge algum problema;*
5. Pessoal responsável pela fiscalização e tratamento dos dados. *Por exemplo, o pessoal que opera e fiscaliza os equipamentos de videogravação; o pessoal que tem direito a consultar o respectivo registo.*
6. O prazo de conservação dos dados tratados devido à fiscalização. De um modo geral, o prazo de conservação dos respectivos dados não ultrapassa seis meses. Salvo exista lei ou normas de contrato que regulam a conservação por um prazo mais longo ou, os dados envolvidos já se tornaram provas de infracções disciplinares, administrativas ou criminais;
7. Especificações sobre os direitos de informação, acesso e oposição, e os princípios que regulam os custos adequados a pagar pelos empregados no exercício do direito de acesso. Os custos reais serão estabelecidos consoante os casos, devendo, no entanto ser comunicado ao empregado antes de exercer o direito de acesso.
8. Estabelecimento das "Regras" para tratamento de assuntos privados pelos empregados quando utilizam as instalações da entidade. Os conteúdos incluem principalmente o seguinte:

   (1). No caso de o empregador permitir que os empregados utilizem o

endereço de correio electrónico, o telefone, visualizem a *internet* da entidade, o tempo autorizado para a utilização e as respectivas restrições, *por exemplo, menção sobre os conteúdos ou tipos que não podem ser transmitidos através do correio electrónico; exigir aos empregados que marquem os correios electrónicos privados com símbolos; regular o exercício de actividades não permitidas aquando da utilização da internet, páginas ou tipos de páginas electrónicas proibidas.*

(2). Zonas onde estão instalados equipamentos de videogravação e o respectivo horário de funcionamento.

(3). As formas de conservar e destruir os respectivos dados.

## 5. Outros assuntos a observar

1. Após ter tomada a decisão de proceder à fiscalização dos empregados, o empregador deve dialogar com os mesmos a propósito do conteúdo da Declaração da recolha de dados pessoais, para se obter a sua compreensão e colaboração.
2. O empregador deve assegurar que o conteúdo da Declaração da recolha de dados pessoais seja conhecido pelos empregados mediante diversos canais, bem como efectuar oportunamente a respectiva revisão e alteração.
3. Estabelecer medidas para a conservação dos dados recolhidos, no sentido de assegurar que os dados não sejam suprimidos, alterados, consultados por pessoas não autorizadas e utilizados para outras finalidades, extraviados ou danificados pela má conservação.
4. Relativamente ao pessoal indicado para fiscalização e tratamento dos dados,

ao mesmo deve ser assegurado formação ética e capacidade técnica, de modo que se cumpra o estipulado na declaração, nomeadamente os objectivos, finalidades e métodos de utilização.

5. Para qualquer zona fiscalizada, os empregados que usam os respectivos equipamentos, e que entram e saem das respectivas zonas devem ter conhecimento do facto de estarem a ser observados e do objectivo da fiscalização, *por exemplo, avisar a pessoa que fez o telefonema após a ligação estabelecida, afixar avisos em locais visíveis na zona com videogravação, e adicionar alerta no correio electrónico.*
6. Caso a fiscalização seja executada por um subcontratante, deve-se escolher um subcontratante que possa proporcionar medidas seguras e garantia de sigilo em domínios de segurança técnica sobre o tratamento de dados, sendo também conveniente que o subcontratante seja restringido também por contrato e instruções.
7. A maior parte das actividades de fiscalização dos empregados refere-se a tratamento automatizado dos dados pessoais , os empregadores devem notificar o Gabinete para a Protecção de Dados Pessoais nos termos do artigo 21.° da Lei da Protecção de Dados Pessoais, devendo esta notificação incluir o conteúdo previsto no artigo 23.° da mesma lei. Caso o tratamento de dados envolva a interconexão de dados pessoais, deve-se solicitar a autorização do Gabinete para a Protecção de Dados Pessoais (artigos 9.° e 22.° da Lei da Protecção de Dados Pessoais).
8. Mesmo que aos empregados seja exigida a não utilização dos equipamentos de entidade para tratamento de assuntos privados, não significa que os empregadores possam fiscalizá-los de acordo com a sua própria vontade. Os empregadores devem cumprir o estabelecido pela Lei da Protecção de Dados

Pessoais quando procederem à fiscalização, e seguir também estas instruções no respectivo tratamento.

9. O Gabinete para a Protecção de Dados Pessoais sugere aos empregadores que tenham condições, a designação de responsável exclusivo para se responsabilizar pelas consultas e exigências sobre o "tratamento de dados pessoais", com vista a garantir da melhor forma os interesses dos empregadores, empregados e destinatários dos serviços.

Este Gabinete procederá ao ajustamento ou revisão apropriada dos princípios subjacentes à elaboração destas instruções de acordo com a situação de aplicação.

O Gabinete para a Protecção de Dados Pessoais

Setembro de 2007

**Anexos:**

1. Minuta: Declaração de Recolha de Dados Pessoais da entidade XXX (Fiscalização das chamadas Telefónicas)
2. Minuta: Declaração de Recolha de Dados Pessoais da entidade XXX (Fiscalização de e-mail e internet)
3. Minuta: Declaração de Recolha de Dados Pessoais da entidade XXX (Fiscalização através de videogravação)

# Declaração de Recolha de Dados Pessoais da entidade XXX (Fiscalização das chamadas Telefónicas)

**(Minuta)**

Esta Declaração, elaborada pela entidade XXX (doravante designada por entidade) é uma declaração da política de fiscalização de chamadas telefónicas realizada no seio da entidade.

## 1. Regras de utilização do telefone da entidade

Devido à necessidade de funcionamento, estão instalados nas instalações da entidade, equipamentos de fiscalização com gravação de chamadas telefónicas.

A entidade permite que os seus trabalhadores utilizem os equipamentos de telefone da entidade por motivos pessoais, no pressuposto de não afectar o funcionamento da entidade, não provocar incómodos ao trabalho, não prejudicar os interesses da entidade e não violar o disposto na lei.

Na utilização de equipamentos da entidade, os trabalhadores não podem exercer as actividades que se seguem:

- Revelação de dados confidenciais ou sensíveis da entidade.
- Exercício de actividades não inseridas nas funções da entidade em nome da mesma.
- Exercício de actividades ilegais.

## 2. Objectivos da fiscalização de chamadas telefónicas

A entidade procederá à fiscalização da utilização do telefone pelos trabalhadores, com os seguintes objectivos:

- Assegurar a qualidade dos serviços prestados;
- Avaliar o desempenho dos trabalhadores
- Garantir os legítimos interesses da entidade.

## 3. Dados pessoais registados por motivo da fiscalização

Devido à necessidade da fiscalização, esta entidade adoptará no sistema telefónico centralizado a correspondente técnica para registar os seguintes tipos de dados: números de telefone emitidos e recebidos pelos trabalhadores, datas, horas de início, horas de conclusão e gravação de conteúdos.

## 4. Utilização de dados pessoais registados por motivo da fiscalização

Para efeitos da fiscalização acima referida, esta entidade pode consultar os dados registados, incluindo auscultar a gravação dos conteúdos da conversa ao telefone.

## 5. Pessoal indicado para fiscalização e tratamento dos dados

Apenas os responsáveis da entidade e os trabalhadores com competência delegada podem consultar os dados supramencionados; todas estas pessoas têm de cumprir o disposto nesta Declaração e, também a obrigação de sigilo.

Para efeitos de investigação disciplinar, os respectivos dados serão eventualmente transferidos para o responsável pela investigação disciplinar.

Para efeitos de investigação sobre crime ou outras infracções, e nos casos em que tem de ser cumprido o disposto na lei, os respectivos dados serão eventualmente transferidos para autoridades judiciais ou policiais criminais, ou outras entidades competentes.

## 6. Prazo de conservação de dados

O prazo de conservação de dados referidos é, normalmente, 6 meses. Para efeitos de investigação sobre crime ou ontras infracções, e nos casos em que se deve cumprir o disposto na lei, os respectivos dados serão possivelmente conservados até 1 mês após a transferência para as autoridades ou entidades referidas no número anterior ou após a sentença transitada em julgado, ou conservados por um prazo mais longo a pedido das mesmas autoridades e entidades.

## 7. Consequências da violação da Declaração

As pessoas que violem esta Declaração podem ser punidas, incluindo a possibilidade de serem despedidas.

## 8. Direitos dos trabalhadores

Os trabalhadores gozam, em conformidade da lei, os direitos de informação, acesso e oposição. Para o exercício do direito de acesso, têm de apresentar, por escrito, o pedido ao responsável da entidade e pagar uma taxa adequada.

**Declaração do Gabinete para a Protecção de Dados Pessoais**

Esta minuta apenas serve de referência. As entidades devem elaborar a própria Declaração de Recolha de Dados Pessoais, de acordo com a situação concreta de tratamento de dados pessoais.

# Declaração de Recolha de Dados Pessoais da entidade XXX
# (Fiscalização de e-mail e internet)
## (Minuta)

Esta Declaração, elaborada pela entidade XXX (adiante designada por entidade) é uma declaração da política de utilização dos equipamentos fornecidos aos seus trabalhadores pela entidade no envio e recepção de e-mail e navegação na internet.

### 1. Regras de envio e recepção de e-mail e navegação na internet

Devido à necessidade do seu funcionamento, a entidade fornece a alguns dos trabalhadores equipamentos para envio e recepção de e-mail e navegação na internet por motivo de trabalho.

A entidade permite aos trabalhadores a utilização dos referidos equipamentos por motivos pessoais nos seguintes casos:

- Condições prévias: não afectar o funcionamento da entidade e o trabalho, não prejudicar os interesses da entidade, não violar o disposto na lei.
- Horário: regra geral, os trabalhadores podem, nos intervalos para descanso, utilizar os equipamentos referidos para tratar de assuntos privados.

Na utilização de e-mail para finalidades privadas, os trabalhadores devem assinalar a referência "privado" nos e-mails destinados à finalidade privada. Os trabalhadores não podem cometer os seguintes actos:

- Emitir e difundir informações indecentes, imorais, maledicentes, insultuosas ou outras informações que violam a lei ou informações criminosas;
- Revelar dados secretos ou sensíveis da entidade;
- Proceder, em nome da entidade, a actividades que não pertencem ao âmbito das funções da entidade;
- Exercer actividades ilegais.

Na navegação na internet para finalidades privadas, os trabalhadores não podem cometer os seguintes actos:

- Navegação nos websites e webpages indecentes ou imorais;
- Descarregar e instalar softwares não autorizados pela entidade;
- Carregar ou difundir dados secretos ou sensíveis que pertencem à entidade;
- Carregar ou difundir informações indecentes, imorais, maledicentes, insultuosas ou outras informações que violam a lei ou informações criminosas;
- Exercer actividades ilegais.

### 2. Objectivos da fiscalização de e-mail e da navegação na internet

A entidade fiscaliza a utilização de e-mail e a navegação na internet pelos

trabalhadores com o seguinte objectivo:

- Assegurar a qualidade dos serviços prestados;
- Avaliar o desempenho dos trabalhadores;
- Garantir a segurança da informação.

## 3. Dados pessoais registados por motivo de fiscalização

Devido à necessidade de fiscalização, a entidade vai utilizar os softwares informáticos e as respectivas tecnologias para registar os tipos de dados apresentados em seguida e depositá-los no seu servidor:

- Os endereços, datas, horas, títulos e conteúdos dos e-mails enviados e recebidos pelos trabalhadores;
- As horas, webpages, informação transmitidas ou recebidas na navegação na internet pelos trabalhadores.

## 4. Utilização dos dados pessoais registados por motivo de fiscalização

Para garantir a qualidade dos serviços prestados e por motivos da avaliação do desempenho dos trabalhadores, a entidade pode consultar, caso necessário, o conteúdo de todos os e-mails nos quais não foi assinalada a referência "privado", depositados na caixa de correio electrónico dos trabalhadores. Para avaliar o desempenho dos trabalhadores, a entidade pode consultar, caso necessário, as horas em que navegaram na internet e as respectivas webpages.

No exame efectuado por motivo de segurança do sistema informático, investigação disciplinar, criminal ou das outras infracções, e noutros casos definidos por lei, a entidade pode, também, consultar o conteúdo dos e-mails assinalados a referência "privado", depositados na caixa de correio electrónico dos trabalhadores, e as informações transmitidas e recebidas pelos trabalhadores.

## 5. Pessoal indicado para fiscalização e tratamento dos dados

Aos trabalhadores com responsabilidade pela gestão da rede da entidade são delegados poderes de consulta dos respectivos registos depositados no servidor da entidade, mas não podem consultar o conteúdo dos e-mails transmitidos ou recebidos pelos trabalhadores. Apenas os responsáveis da entidade e as pessoas com competência delegada podem consultar todos os registos incluindo o referido conteúdo dos e-mails e informações transmitidas e recebidas pelos trabalhadores. Todas estas pessoas têm de cumprir o disposto nesta Declaração e a obrigação de sigilo.

Para efeitos de investigação disciplinar, os respectivos dados serão eventualmente transferidos para o responsável pela investigação disciplinar.

Para efeitos de investigação sobre crime ou outras infracções, e nos casos em que

tem de ser cumprido o disposto na lei, os respectivos dados serão eventualmente transferidos para autoridades judiciais ou policiais criminais, ou outras entidades competentes.

## 6. Prazo de conservação dos dados

O prazo de conservação de dados referidos é, normalmente, 6 meses. Para efeitos de investigação sobre crime ou outras infracções, e nos casos em que se deve cumprir o disposto na lei, os respectivos dados serão possivelmente conservados até 1 mês após a transferência para as autoridades ou entidades referidas no número anterior ou após a sentença transitada em julgado, ou conservados por um prazo mais longo a pedido das mesmas autoridades e entidades.

## 7. Consequências da violação da Declaração

As pessoas que violem esta Declaração podem ser punidas, incluindo a possibilidade de serem despedidas.

## 8. Direitos dos trabalhadores

Os trabalhadores gozam, em conformidade com a lei, dos direitos de informação, acesso e oposição. Para o exercício do direito de acesso, têm de apresentar, por escrito, o pedido ao responsável da entidade e pagar uma taxa adequada.

**Declaração do Gabinete para a Protecção de Dados Pessoais**

Esta minuta apenas serve de referência. As entidades devem elaborar a própria Declaração de Recolha de Dados Pessoais, de acordo com a situação concreta de tratamento de dados pessoais.

# Declaração de Recolha de Dados Pessoais da entidade XXX
# (Fiscalização através de videogravação)
## (Minuta)

Esta Declaração, elaborada pela entidade XXX (adiante designada por entidade) é uma declaração da política de fiscalização através de videogravação nas suas instalações.

### 1. Fiscalização através de videogravação

Devido à necessidade do seu funcionamento, a entidade mandou instalar, nas suas instalações, equipamentos de videogravação para a fiscalização.

Os equipamentos foram instalados em locais de atendimento ao público (incluindo a gravação de som em simultâneo), entradas e saídas dos gabinetes e armazéns, corredores, funcionando automaticamente de um modo geral durante todo o dia.

### 2. Objectivos da fiscalização através de videogravação

A fiscalização através de videogravação a efectuar no seio da entidade tem os seguintes objectivos:

- Garantir o património da entidade e outros interesses legais;
- Garantir a segurança dos trabalhadores e outros legítimos direitos e interesses;
- Assegurar a qualidade dos serviços prestados (apenas na área de atendimento ao público);
- Avaliar o desempenho dos trabalhadores (apenas em locais de atendimento ao público, entrada e saída, incluindo a área em frente do sítio onde se situa a máquina de registo de assiduidade).

### 3. Dados pessoais registados por motivo de fiscalização

Devido à necessidade de fiscalização, os equipamentos de videogravação para a fiscalização desta entidade vão registar automaticamente, mediante as respectivas tecnologias, todas as imagens que apareçam nas suas lentes (sendo simultaneamente gravado o som em alguns casos), a data e hora correspondentes.

### 4. Utilização dos dados pessoais registados por motivo de fiscalização

Para as finalidades da fiscalização referidas, a entidade pode consultar os dados registados, incluindo os sons e imagens gravados.

## 5. Pessoal indicado para fiscalização e tratamento dos dados

Os trabalhadores com responsabilidade pela suprevisão da segurança são delegados poderes de consulta imediata dos referidos dados gravados, mas não podem consultar, repetidamente, os sons e imagens gravados anteriormente. Apenas os responsáveis da entidade e os trabalhadores com competência delegada podem consultar os referidos dados incluindo os sons e imagens gravados anteriormente. Todas estas pessoas têm de cumprir o disposto nesta declaração e a obrigação de sigilo.

Para efeitos de investigação disciplinar, os respectivos dados serão eventualmente transferidos para o responsável pela investigação disciplinar.

Para efeitos de investigação criminal e nos casos em que tem de ser cumprido o disposto na lei, os respectivos dados serão eventualmente transferidos para autoridades judiciais ou policiais criminais, ou outras entidades competentes.

## 6. Prazo de conservação dos dados

O prazo de conservação de dados referidos é, normalmente, 6 meses. Para efeitos de investigação sobre crimes e outras infracções, e nos casos em que se deve cumprir o disposto na lei, os respectivos dados serão possivelmente conservados até 1 mês após a transferência para as autoridades ou entidades referidas no número anterior ou após a sentença transitada em julgado, ou conservados por um prazo mais longo a pedido das mesmas autoridades e entidades.

## 7. Consequências da violação da Declaração

As pessoas que violem esta Declaração podem ser punidas, incluindo a possibilidade de serem despedidas.

## 8. Direitos dos trabalhadores

Os trabalhadores gozam, em conformidade com a lei, dos direitos de informação, acesso e oposição. Para o exercício do direito de acesso, têm de apresentar, por escrito, o pedido ao responsável da entidade e pagar uma taxa adequada.

**Declaração do Gabinete para a Protecção de Dados Pessoais**

Esta minuta apenas serve de referência. As entidades devem elaborar a própria Declaração de Recolha de Dados Pessoais, de acordo com a situação concreta de tratamento de dados pessoais.