



IFAP

Instituto de Financiamento
da Agricultura e Pescas, IP

AVALIAÇÃO DE IMPACTO NA PROTEÇÃO DE DADOS (AIPD)

Recolha de Dados Biométricos Faciais



**REPÚBLICA
PORTUGUESA**

AGRICULTURA
E ALIMENTAÇÃO

IP – Informação Pública

FICHA TÉCNICA

Título

Avaliação de Impacto na Proteção de Dados (AIPD) - Recolha de Registo Biométrico facial

Versão 2

Autor/Editor

IFAP - Instituto de Financiamento da Agricultura e Pescas, I.P.

R. Castilho, nº 45 - 51 1269-164 LISBOA

Tel. 21 384 60 00 * Fax: 21 384 61 70

Website: www.ifap.pt * E-mail: ifap@ifap.pt

Conceção Técnica:

DGR/UORH

Nome e contactos do DPO:

João Pinto

Endereço de Correio eletrónico: dpo@ifap.pt

Telefone: 21 384 60 57 | Ext. 12021

Comunicação escrita dirigida ao Encarregado da Proteção de Dados para:

Rua Castilho, n.º 45-51, 1269-164 LISBOA

Data de Edição

19-10-2023

ÍNDICE

1. ENQUADRAMENTO	5
2. PROCESSO DE TRATAMENTO DOS DADOS BIOMÉTRICOS FACIAIS	7
2.1. FINALIDADE, CONTEXTO E PROPÓSITO DO TRATAMENTO	7
2.2. DESCRIÇÃO FUNCIONAL DA OPERAÇÃO DE TRATAMENTO	7
2.3. ÂMBITO DO TRATAMENTO	10
2.4. ATIVOS INFORMÁTICOS ASSOCIADOS AO TRATAMENTO	11
3. AVALIAÇÃO DA NECESSIDADE E PROPORCIONALIDADE	13
4. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS	18
5. PARECER DO DPO	19
6. PARECER DA COMISSÃO DE TRABALHADORES	19

1. ENQUADRAMENTO

O IFAP, I.P (IFAP) dispõe de um sistema de controlo biométrico de assiduidade, já objeto da autorização n.º 3049/2009, da CNPD, que, a par do número de trabalhador, exige a imposição da impressão digital no relógio de ponto, o que poderá representar um risco para a saúde dos trabalhadores, tendo em conta que obriga ao contacto físico com o equipamento.

Neste contexto, surgiu a necessidade do IFAP implementar um novo sistema de controlo biométrico de assiduidade por reconhecimento facial, totalmente seguro para a saúde dos trabalhadores, uma vez que não envolve qualquer contacto físico com o relógio de ponto.

O Regulamento Geral sobre a Proteção de Dados (RGPD), pelo n.º 1 do seu artigo 9.º, proíbe o tratamento de dados biométricos para identificar uma pessoa de forma inequívoca, exceto nos casos especificamente previstos no n.º 2 desse artigo, o qual pressupõe a existência de uma lei ou convenção coletiva que cumpra os requisitos legais e o admita.

A Lei 58/2019, no n.º 6 do artigo 28.º, prevê que “O tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados.”

Por sua vez, o artigo 35.º do RGPD obriga a que o responsável pelo tratamento, no caso de dados sensíveis, proceda, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas, sobre a proteção de dados pessoais, quando um certo tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, pela sua natureza, âmbito, contexto e finalidades.

Por outro lado, a Comissão Nacional de Proteção de Dados (CNPD) também obriga à realização de uma AIPD, sempre que haja alteração das condições autorizadas para o funcionamento do sistema biométrico.

A presente Avaliação de Impacto sobre a Proteção de Dados (AIPD) tem como objetivo verificar a conformidade com o RGPD do novo sistema de controlo biométrico de assiduidade por reconhecimento facial, que irá ser implementado pelo IFAP, deixando de ser necessária a autorização da CNPD, conforme o n.º 2 do artigo 62º da Lei n.º 58/2019.

Foram considerados os seguintes documentos na elaboração da presente AIPD:

- Autorização n.º 3049/2009 da CNPD - Apreciação jurídica do tratamento de dados biométricos (impressão digital);
- Princípios sobre a utilização de Dados Biométricos no âmbito do controlo de acessos e de assiduidade da CNPD;
- Parecer 20/2018 da CNPD;
- Orientações do Grupo de Trabalho do Artigo 29º da Diretiva 95/46/CE relativas à Avaliação de Impacto e a Proteção de Dados (AIPD) e que determinam se o tratamento é “suscetível de resultar num elevado risco” para efeitos do Regulamento 2016/67917/PTWP 248, versão 01, revistas e adotadas em 4 de outubro de 2017.
- Revista Científica sobre *Cyberlaw* do Centro de Investigação Jurídica do Ciberespaço - CIJIC - da Faculdade de Direito da Universidade de Lisboa - edição N.º VII - maio de 2019 - Avaliação

de Impacto na Proteção de Dados - Tabela 1 - Passos do Modelo AIPD da “Information Commissioner’s Office (ICO)”.

- NP - ID - Avaliação de Impacto sobre a Proteção de Dados, em vigor;
- Requisitos de integração entre sistemas de relógio de ponto e o sistema de gestão de tempos SIAG;
- Documento de apoio facultado pelo DPO do IFAP e que contem uma síntese das orientações que sobre esta matéria foram produzidas pelo Comité Europeu para a Proteção de Dados;
- Informação n.º 07043/2023- Análise de proposta de divulgação geral - controlo de assiduidade - recolha de dados biométricos de reconhecimento facial.

2. PROCESSO DE TRATAMENTO DOS DADOS BIOMÉTRICOS FACIAIS

2.1. Finalidade, contexto e propósito do tratamento

A finalidade do tratamento dos dados biométricos assenta na necessidade de facilitar o cumprimento de um objetivo que a lei reconhece integrar-se no âmbito dos poderes de controlo da entidade responsável pelo tratamento: a fixação do horário de trabalho, o controlo da assiduidade e o registo do tempo de trabalho.

Efetivamente, a Lei Geral do Trabalho em Funções Públicas, aprovada em anexo à Lei n.º 35/2014, de 20 de junho, obriga ao registo dos tempos de trabalho, sendo obrigatório esse registo ser efetuado por sistemas automáticos, nos órgãos ou serviços com mais de 50 trabalhadores.

A recolha dos dados biométricos de reconhecimento facial tem como único objetivo o registo de marcações de tempo de trabalho para o controlo de assiduidade, tratados no âmbito da relação laboral estabelecida entre o IFAP (responsável pelo tratamento) e o trabalhador (titular dos dados).

Os interesses legítimos subjacentes ao tratamento dos dados biométricos faciais dos trabalhadores pelo IFAP estão estabelecidos na Lei n.º 58/2019, que assegura a aplicação do RGPD na ordem jurídica portuguesa. Por sua vez, a Deliberação n.º 410/2023, publicada no Diário da República, delega nos dirigentes do IFAP as competências relativas ao responsável pelo tratamento de dados pessoais, na aceção e nos termos da Lei n.º 58/2019.

O IFAP também dispõe de um Código de Ética e Conduta que inclui um ponto relativo à proteção de dados e estabelece que o tratamento de dados pessoais no IFAP deve cumprir os princípios definidos no RGPD, designadamente: ser lícito, leal e transparente em relação aos titulares dos dados, ser executado exclusivamente no âmbito das atividades de tratamento e para as finalidades determinadas pelo IFAP.

2.2. Descrição funcional da operação de tratamento

Descreve-se, de seguida, o modo de funcionamento do sistema biométrico dos relógios de ponto.

- **Recolha dos dados biométricos dos trabalhadores**

O trabalhador com privilégios inerentes às funções de gestão de assiduidade que vai recolher o dado biométrico insere o “Número do Trabalhador” e a unidade orgânica a que o trabalhador está afeto na base de dados associada ao relógio de ponto.

O trabalhador posiciona-se em frente ao relógio de ponto no momento da recolha do dado biométrico.

O sistema recolhe uma amostra da característica biométrica da face (*template*) através de um sensor analógico e transforma a amostra em código matemático encriptado (chave primária).

Tendo em conta que, isoladamente, o código matemático encriptado (ID Utilizador) não identifica o trabalhador é necessário recolher e associar o dado pessoal “N.º Trabalhador”.

O “ID Utilizador” (chave primária), o “Número de Trabalhador” e a unidade orgânica são guardados na base de dados de controlo de assiduidade associada aos relógios de ponto”.

O registo da unidade orgânica na base de dados afigura-se indispensável, na medida em que o IFAP dispõe de edifícios localizados em moradas diferentes.

- **Registo das marcações de tempo dos trabalhadores**

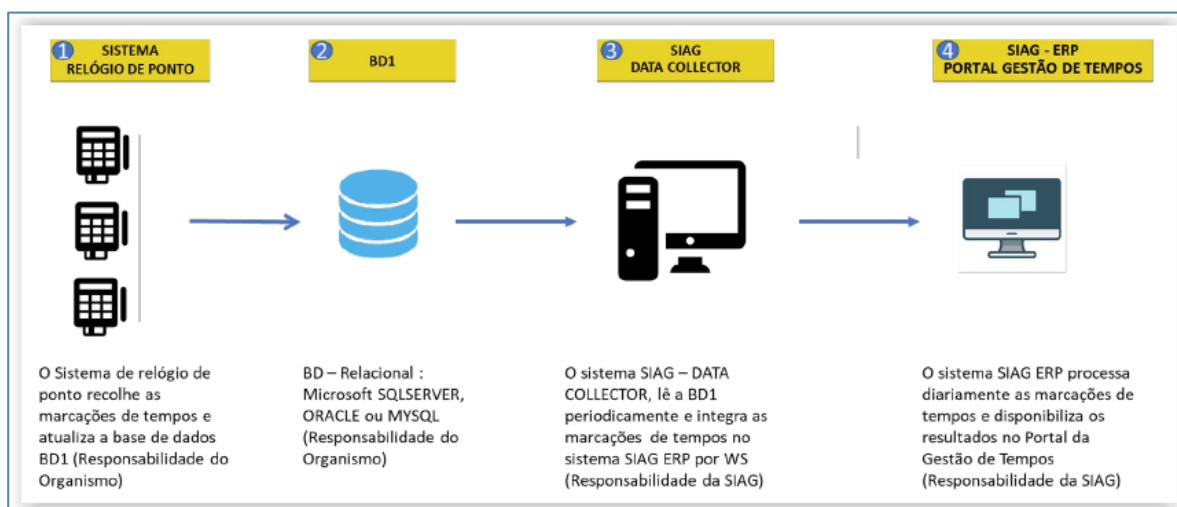
O processo de identificação é um processo de combinação de um-para-muitos (1:N) ou seja:

Sempre que o trabalhador se posiciona em frente ao relógio de ponto para verificar a sua identidade, uma nova amostra biométrica facial é capturada pelo sensor. A informação analógica do sensor é então convertida para a sua representação digital (*template*). Em seguida, esta representação digital é comparada com os *templates* biométricos armazenados e se coincidir com um dos guardados e encriptados (chave primária) é registada a marcação do tempo do trabalhador na base de dados de controlo de assiduidade associada aos relógios de ponto, através da chave primária associada ao “Número do Trabalhador”.

Por sua vez, os registos de marcações de tempos serão integrados, de forma automática, no sistema de gestão de tempos SIAG que está a ser implementado no IFAP.

O sistema SIAG fará a leitura à base de dados de controlo de assiduidade associada aos relógios de ponto (BD1) de forma sequencial, sempre a partir da última leitura em termos cronológicos e faz uma cópia integral dessa leitura.

O diagrama seguinte descreve, de forma simples, como é feita a integração da base de dados de controlo de assiduidade associada aos relógios de ponto com o sistema SIAG:



- **Consulta aos dados biométricos faciais**

Os dados biométricos faciais dos trabalhadores não podem ser consultados, uma vez que são transformados em código matemático encriptado (chave primária), de forma a impossibilitar a reprodução das características biométricas (irreversibilidade dos dados).

Por sua vez, a base de dados de controlo de assiduidade associada aos relógios de ponto, onde é guardado o código matemático encriptado, o “N.º de Trabalhador” e os respetivos registos de entrada e saída, apenas pode ser acedida pelos trabalhadores com privilégios inerentes às funções de gestão de assiduidade, respeitando os princípios e regras definidas no âmbito do Sistema da Segurança de Informação:

✓ OS - Controlo de Acessos

No que respeita ao controlo de acesso a sistemas aplicativos e gestão de privilégios;

✓ OS - Classificação e Manuseamento da Informação

A informação disponibilizada pela base de dados de controlo de assiduidade associada aos relógios de ponto é tratada respeitando o nível de segurança adequado ao seu tratamento (IC - Informação Condicionada).

• **Conservação dos dados na base de dados de controlo de assiduidade associada aos relógios de ponto**

O dado biométrico encriptado de cada trabalhador, o respetivo “Número de Trabalhador” e a “Localização do terminal biométrico e IP” são guardados na base de dados de controlo de assiduidade associada aos relógios de ponto até ao momento em que ocorra a transferência do trabalhador para outra entidade ou enquanto durar o vínculo laboral do trabalhador com o IFAP.

Estes dados serão eliminados manualmente na base de dados de controlo de assiduidade associada aos relógios de ponto pelos trabalhadores com privilégios inerentes às funções de gestão de assiduidade.

Os restantes dados que constam na base de dados de controlo de assiduidade associada aos relógios de ponto, serão eliminados a definir pelo IFAP.

2.3. Âmbito do tratamento

Natureza dos dados	Dados de categorias especiais - dados biométricos por reconhecimento facial.
Quantidade de dados coletados e usados	Dados guardados no relógio de ponto: • <i>Template</i> - Representação digital dos pontos fisiométricos da face que é transformado em código matemático encriptado para identificar o trabalhador em associação ao “N.º de Trabalhador”. Dados guardados na base de dados de controlo de assiduidade associada aos relógios de ponto: • ID Utilizador - Código matemático encriptado resultante do processo de algoritimização dos pontos fisiométricos da face de cada trabalhador (chave primária), que isoladamente não permite identificar o trabalhador; • Número do Trabalhador - dado pessoal, que é associado ao “ID Utilizador” para permitir a identificação do trabalhador; • Unidade Orgânica a que o trabalhador está afeto; • Data e hora da picagem - dado utilizado para registo das marcações de tempo, no âmbito do controlo de assiduidade; • Localização do terminal biométrico e IP - dado que permite identificar a localização do posto de trabalho do trabalhador, decorrente de orientação do DGR âmbito do controlo da assiduidade.
Frequência no tratamento	Sempre que o trabalhador interage com o relógio de ponto.
Duração do armazenamento	O dado biométrico encriptado de cada trabalhador, o respetivo “Número de Trabalhador” e a “Localização do terminal biométrico e IP” são guardados na base de dados de controlo de assiduidade associada aos relógios de ponto até ao momento em que ocorra a transferência do trabalhador para outra entidade ou enquanto durar o vínculo laboral do trabalhador com o IFAP. Os restantes dados são eliminados automaticamente da base de dados de controlo de assiduidade associada aos relógios de ponto com a periodicidade a definir pelo IFAP.
Número de titulares abrangidos	Os titulares dos dados são os trabalhadores ativos do IFAP que não exercem funções de dirigente, uma vez que a esta função está legalmente atribuída a isenção de horário.
Área geográfica onde o tratamento ocorre	Rua Castilho 45/51 - Lisboa Rua Fernando Curado Ribeiro 4G e 4 A - Lisboa Rua Vasco da Gama, 7 - Prior Velho

2.4. Ativos informáticos associados ao tratamento

Os dados biométricos faciais dos trabalhadores serão tratados em seis equipamentos de relógio de ponto, com as seguintes características técnicas:

- ✓ Biometrias Faciais: superior a 1.000 (1:N);
- ✓ Utilizadores/Impressões Digitais: Não;
- ✓ Cartão: Sim;

São também necessários os seguintes requisitos de instalação do software:

- ✓ Servidor de base de dados SQL Server 2012, com mínimo de 8 GB de memória e 100GB de disco livre;
- ✓ Servidor aplicacional residente no IFAP necessário à implementação da solução; (máquina virtual com sistema operativo Windows Server 2012 R2, com mínimo de 8 GB de memória e 100GB de disco livre);
- ✓ Base de dados MS SQL Server 2012 (BD1) residente no IFAP;
- ✓ PC's DeskTop por utilizador CPU Core i3 com mínimo de 4GB de memória, sistema operativo Windows 8.1 ou superior e 20GB de disco livre)
- ✓ 1 PC DeskTop CPU Core i5 com mínimo de 4GB de memória, sistema operativo Windows 8.1 ou superior e 20GB de disco livre e com a instalação de utilitários de acesso ao SQL Server para efeitos de manutenção corretiva;
- ✓ Rede ethernet entre servidores, PC's Desktop e terminais de picagem;
- ✓ Licenças de software necessárias, nomeadamente Windows Sever, SQL Server e CAL's para cada PC DeskTop;
- ✓ Atribuição de gama de IP's reservada para os terminais.
- ✓ A solução deve integrar com balanceadores de carga (F5 BigIP) através de URL do tipo <https://int.ifap.pt/aplicacao> e deve disponibilizar os métodos necessário para o balanceador validar a disponibilidade dos serviços aplicacionais (por exemplo respondendo a keepalive com 200 OK);
- ✓ A solução deve ser compatível/suportar as politicas de segurança de rede impostas e definidas na solução Cisco ISE (NAC);
- ✓ Compatibilidade da solução proposta com versões atuais dos principais browsers (MS edge, Chrome, Firefox), ao longo da vigência do contrato
- ✓ A solução deverá garantir a comunicação segura entre terminais/pantómetros e bases de dados (encriptação e protocolos seguros);
- ✓ A solução deverá garantir a comunicação segura entre interfaces aplicacionais e bases de dados (encriptação e protocolos seguros).

O servidor aplicacional e a base de dados de controlo de assiduidade associada aos relógios de ponto estão sujeitos às regras de segurança contra *function creep* estabelecidas no IFAP para todos os sistemas de informação.

Por outro lado, o IFAP garante a realização de um *backup* diário ao servidor aplicacional da solução, com uma retenção de curta duração (3 meses).

Também são garantidos *backups* à base de dados de controlo de assiduidade associada aos relógios ponto através da implementação de automatismos para a sua realização para disco e com uma rotação de 3 dias.

Desta forma, o IFAP garante que são adotados os princípios e regras definidos no âmbito da Segurança dos Sistemas de Informação estabelecidos na “OS - Cópias de Segurança”.

De realçar que a instalação dos equipamentos de relógio de ponto também cumpre as regras estabelecidas na “OS - Segurança Física e Ambiental de Infraestruturas e Equipamentos”.

Os relógios de ponto estão instalados nas portarias dos edifícios do IFAP, reduzindo os riscos de ameaças ambientais, e de forma a poderem ser controlados pelos elementos da empresa que presta o serviço de segurança ao IFAP, diminuindo os riscos de acessos não autorizados.

Fica também impedido o uso dos relógios de ponto como meio de controlar a circulação de trabalhadores no interior das instalações do IFAP.

Importa ainda salientar que nos edifícios da Castilho e do Campo Grande onde estão instalados dois equipamentos, os mesmos estão localizados com respeito pelas regras de distanciamento físico recomendadas pela Direção Geral de Saúde (DGS).

De salientar que o IFAP está certificado pela entidade APCER no âmbito dos sistemas de gestão de segurança de informação, de acordo com o referencial ISO/IEC 27001, que obriga o Instituto a adotar um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação (SGSI).

A adoção das práticas de gestão documentadas na norma acima referida representa um conjunto de benefícios, nomeadamente, no que respeita aos princípios da confidencialidade, integridade e disponibilidade da informação.

3. AVALIAÇÃO DA NECESSIDADE E PROPORCIONALIDADE

O RGPD determina que sejam previstas medidas para demonstrar a necessidade e proporcionalidade do tratamento dos dados relativamente ao objetivo e a sua conformidade com o Regulamento [(artigo 35º, n.º 7, alíneas b) e d) e “Considerando (90)” do RGPD].

Na implementação do novo sistema biométrico serão adotadas medidas para fazer face aos riscos, incluindo as medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e que demonstram a conformidade com o RGPD, tendo em conta os direitos e os interesses legítimos dos trabalhadores que são os titulares dos dados.

- **Proporcionalidade e necessidade do tratamento dos dados**

O registo dos tempos de trabalho, através de sistemas biométricos apresenta vantagens de segurança, comparativamente aos meios tradicionais, uma vez que não implica a utilização de códigos ou cartões que podem ser esquecidos ou serem alvo de apropriação ilícita.

No caso do IFAP estas vantagens já eram asseguradas pelo sistema biométrico por impressão digital.

O sistema biométrico por reconhecimento facial irá trazer vantagens de segurança ao nível da saúde pública, porque evita o contacto direto dos trabalhadores com os relógios de ponto, não afetando a sua integridade física atenta a forma como os elementos da identidade são captados.

Na prossecução de interesses legítimos do responsável pelo tratamento, de acordo com a alínea f) do n.º 1 do artigo 6º do RGPD, os dados biométricos faciais dos trabalhadores serão tratados apenas para a finalidade de registo de marcações de tempo de trabalho no âmbito do controlo de assiduidade, não sendo, portanto, necessário o consentimento prévio do trabalhador.

Não obstante ser dispensável o consentimento do titular dos dados, de acordo com o n.º 9 do artigo 35º do RGPD, antes da entrada em funcionamento do sistema biométrico facial, será solicitada consulta à Comissão de Trabalhadores do IFAP, enquanto representante dos titulares dos dados.

Fica assegurado o cumprimento da alínea f) do n.º 1 do artigo 6º, da alínea a) do n.º 1 do artigo 5º e da alínea b) do n.º 2 do artigo 9º do RGPD.

O sistema biométrico regista apenas uma representação digital (*template*) dos dados biométricos faciais recolhidos e faz a sua encriptação, ficando assim assegurada a irreversibilidade dos dados, por forma a que não possam ser tratados com propósito diferente da finalidade para que são recolhidos, ou seja, o controlo da assiduidade.

Neste sentido, considera-se preenchida a exigência de minimização dos dados tratados, porquanto são os adequados, pertinentes e limitados ao que é necessário relativamente à finalidade para a qual são tratados.

Fica assim assegurado o cumprimento das alíneas b) e c) do n.º 1 do artigo 5º do RGPD.

Também é assegurado o cumprimento da alínea e) do n.º 1 do artigo 5º do RGPD, na medida em que o dado biométrico não é guardado.

O código matemático (chave primária) resultante da interpretação algorítmica da respetiva representação digital é guardado na base de dados de controlo de assiduidade associada aos relógios de pontos.

O dado biométrico encriptado do trabalhador será conservado apenas durante o período necessário para a prossecução das finalidades do tratamento a que se destinam, ou seja, será eliminado se ocorrer uma transferência do trabalhador para outra entidade ou no momento da cessação do vínculo laboral com o IFAP.

Para o efeito, o Modelo “IFAP-0808.XX.TP - Pedido de Criação/Alteração/Cessação do Posto de Trabalho” contempla a necessidade de desativação do perfil “RH” do trabalhador, por motivos de mobilidade ou cessação do vínculo laboral com o IFAP.

Fica assim assegurado o cumprimento da alínea e) do n.º 1 do artigo 5º do RGPD.

De forma a cumprir as regras e limites estabelecidos pela CNPD, o responsável pelo tratamento, antes da entrada em vigor do novo sistema biométrico, assegura a eliminação da base de dados de controlo de assiduidade associada ao sistema biométrico por impressão digital, objeto da autorização n.º 3049/2009 da CNPD.

- **Direitos dos Titulares dos dados:**

No tratamento dos dados biométricos dos trabalhadores serão adotadas medidas que contribuem para os direitos dos titulares dos dados:

- ✓ Informações fornecidas aos titulares dos dados (artigos 12º e 13º do RGPD)

Os trabalhadores serão informados, por Divulgação Geral, de forma clara, concisa e transparente, sobre:

- as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- o interesse legítimo do responsável pelo tratamento, em razão do qual o titular dos dados está obrigado a fornecer os dados pessoais, bem como sobre as eventuais consequências de não fornecer esses dados;
- os direitos dos titulares;
- o prazo de conservação dos dados;
- os contactos do encarregado da proteção de dados;
- o direito de apresentar reclamação a uma autoridade de controlo;
- a entrada em funcionamento do sistema biométrico facial, que se prevê no primeiro dia do mês seguinte ao da Divulgação.

O trabalhador pode exercer os seguintes direitos:

- ✓ Acesso aos dados pessoais (artigo 15º do RGPD);

Os trabalhadores podem aceder aos seus dados pessoais guardados na base de dados de controlo de assiduidade associada aos relógios de ponto.

Para o efeito, o trabalhador deve dirigir-se ao DGR/UORH através de mensagem eletrónica para o endereço “Interno.Assiduidade@ifap.pt”.

O trabalhador também pode aceder às informações que constam no n.º 1 do citado artigo, através da consulta da presente AIPD, que será anexada à Divulgação Geral aos trabalhadores antes da entrada em funcionamento do sistema biométrico facial.

✓ Retificação dos dados (artigo 16º do RGPD)

O trabalhador tem o direito de solicitar a retificação dos dados ao responsável pelo tratamento, caso não se apresentem conformes.

Para o efeito, o trabalhador deve dirigir-se ao DGR/UORH através de mensagem eletrónica para o endereço “Interno.Assiduidade@ifap.pt”.

Enquanto o responsável pelo tratamento dos dados não concluir a retificação solicitada, o trabalhador efetua o registo dos tempos de trabalho através da leitura de um cartão pelo relógio de ponto.

✓ Limitação do tratamento (artigo 18º do RGPD)

Tendo em consideração o fundamento de licitude para a finalidade da recolha dos dados biométricos faciais, não se aplica o direito à limitação do tratamento dos dados pessoais.

✓ Direito de oposição (artigo 21º do RGPD)

Quando existam razões ponderosas e legítimas relativas à situação particular do titular dos dados, este pode exercer o direito de oposição, em relação ao tratamento.

Neste caso, deve apresentar os fundamentos em que assenta o direito de oposição, cabendo ao responsável pelo tratamento apreciá-los e decidir sobre a sua pertinência.

Para o efeito, o trabalhador deve dirigir-se ao DGR/UORH através de mensagem eletrónica para o endereço “Interno.Assiduidade@ifap.pt”.

Se após a apreciação dos fundamentos apresentados o responsável pelo tratamento decidir que estes são pertinentes, o trabalhador passa a efetuar o registo dos tempos de trabalho através da leitura de um cartão pelo relógio de ponto.

✓ Apagamento dos dados (alínea c) do n.º 1 do artigo 17º)

Tendo em consideração o fundamento de licitude para a finalidade da recolha dos dados biométricos faciais, não se aplica o direito ao apagamento dos dados pessoais.

Consistindo os dados biométricos faciais num *template* (representação digital de pontos fisiométricos da face) e dada a sua característica de irreversibilidade, é tecnicamente inviável o exercício dos seguintes direitos, no âmbito do RGPD:

✓ Portabilidade dos dados (artigo 20º)

Não são aplicáveis os seguintes direitos:

✓ Relações com os subcontratantes (artigo 28º)

Os dados biométricos serão tratados exclusivamente pelo IFAP.

✓ Consulta prévia (artigo 36º)

O responsável pelo tratamento dos dados consulta previamente a autoridade de controlo quando da avaliação dos dados sujeitos a tratamento resultar um elevado risco para o seu titular, o que não se considera pela análise realizada.

O tratamento dos dados biométricos faciais é legalmente sustentado nos seguintes termos:

✓ Regulamento Geral da Proteção de Dados (RGPD)

A licitude do tratamento dos dados, definida no RGPD, é respeitada, porquanto se insere na alínea f) do n.º 1 do artigo 6º que permite o tratamento de dados pessoais se o mesmo for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento, não sendo necessário o consentimento prévio do trabalhador.

A alínea b) do n.º 2 do artigo 9.º do RGPD permite o tratamento de dados biométricos para identificar uma pessoa de forma inequívoca se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados.

✓ Lei Geral do Trabalho em Funções Públicas (LTFP)

O artigo 104º da Lei n.º 35/2014 obriga ao registo do número de horas prestadas pelo trabalhador, por dia e por semana, com indicação da hora de início e termo de trabalho, bem como dos intervalos efetuados.

Este registo é obrigatoriamente efetuado por mecanismos automáticos quando o serviço tenha mais de 50 trabalhadores.

✓ Código de Trabalho

O artigo 18º permite o tratamento de dados biométricos se forem necessários, adequados e proporcionais aos objetivos a atingir e conservados durante o período necessário para prossecução das finalidades do tratamento a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outra entidade ou da cessação do vínculo laboral com o IFAP.

✓ Lei da Proteção de Dados Pessoais

O n.º 1 do artigo 28º da Lei n.º 58/2019 permite que o empregador trate os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código de Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no mesmo artigo.

O n.º 6 do artigo 28º da Lei n.º 58/2019 considera legítimo o tratamento de dados biométricos do trabalhador para efeitos de controlo de assiduidade, devendo assegurar-se que apenas sejam utilizadas representações dos dados biométricos e que o respetivo processo de recolha não permita a respetiva reversibilidade.

✓ Deliberação n.º 410/2023 publicada no Diário da República n.º 75/2023, Série II de 2023-04-17

Deliberação que delega nos dirigentes do IFAP as competências relativas ao responsável pelo tratamento de dados pessoais, na aceção e nos termos da Lei n.º 58/2019, que assegura a execução, na ordem jurídica nacional do Regulamento (EU) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016 (RGPD).

4. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Os mecanismos de criptografia visam proteger a informação (documentos, dados, transações online, palavras-chave, etc.) do acesso ou alteração por pessoas não autorizadas para o efeito, utilizando algoritmos (cifras) e chaves para converter os dados legíveis para um formato não compreensível.

No caso do tratamento dos dados biométricos faciais dos trabalhadores que são alvo da presente avaliação de impacto à proteção de dados, também é garantida a sua irreversibilidade, ou seja, não é possível decifrar os dados encriptados, o que torna impossível a sua utilização para propósitos diferentes do registo de tempos de trabalho.

Deste modo, consideram-se mitigados os riscos de:

- usurpação da identidade de trabalhadores através do acesso indevido aos seus dados biométricos;
- utilização da identidade usurpada para acesso indevido aos sistemas de informação e/ou espaços físicos (que utilizem este tipo de controlo biométrico).

Em caso de ocorrência sucessiva de falsas leituras (rejeições ou aceitações) do dado biométrico, o sistema permite o registo dos tempos de trabalho através da leitura de um cartão pelo relógio de ponto.

Assim, na eventualidade de acesso ilegítimo, de modificação indesejada, de desaparecimento dos dados, ou de falhas de sistema, considera-se que o risco não tem expressão significativa nos direitos e liberdades dos trabalhadores do IFAP.

O tratamento dos dados biométricos faciais será implementado por uma empresa de referência no mercado português, com vasta experiência no desenvolvimento deste tipo de soluções.

Dado o exposto, prevê-se que o novo sistema apresente um elevado grau de desempenho (*performance*), de eficiência e de segurança (fiabilidade), considerando-se dispensável a realização de um projeto piloto com uma amostra de utilizadores para validação do sistema.

5. PARECER DO DPO

De acordo com o n.º 2 do artigo 35º do RGPD foi solicitado o parecer do encarregado de proteção de dados do IFAP (DPO) que concordou com o teor da presente AIPD.

6. PARECER DA COMISSÃO DE TRABALHADORES

De acordo com o n.º 9 do artigo 35º do RGPD foi efetuada a consulta à Comissão de Trabalhadores do IFAP na qualidade de representantes dos titulares dos dados, que concordou com os termos da presente AIPD.