
# Definições e Conceitos

Regulamento Geral Sobre a Proteção de Dados (RGPD)

O **"titular dos dados "**é uma pessoa singular (aluno, trabalhador, visitante, outros) que pode ser identificada, direta ou indiretamente e cujos dados são objeto de tratamento por parte do responsável pelo tratamento (no caso IPV) ou subcontratante(exº empresa de medicina do trabalho)

Os **"destinatários "**são pessoas singulares ou coletivas que recebem comunicações de dados de caráter pessoal. Assim os destinatários podem ser simplesmente os alunos, titulares de responsabilidade parental, trabalhadores do IPV, visitantes, entidades internas(Escolas/Serviços) ou externas tanto privadas, como públicas (CGA, Segurança Social, etc);

**"dados pessoais "**- informações relativas a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa que possa ser identificada direta ou indiretamente;

**Exemplos:**

**biográficos:** Nome, data de nascimento, sexo, naturalidade, nacionalidade, filiação, estado civil, fotografia, assinatura, informação sobre o agregado familiar, etc.

**dados de saúde:** boletim de vacinas, atestados médicos, relatórios médicos, número de beneficiário de sistema de saúde, número de identificação da segurança social da ADSE, etc

**"dados pessoais enriquecidos ",** por oposição aos dados pessoais originais (brutos), são dados gerados pelo responsável pelo tratamento(IPV) ou subcontratante (exº empresa da medicina no trabalho) ou resultantes de uma análise ou dedução acerca dos dados em bruto;

**"tratamento "-** uma operação ou conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não, tais como a recolha, o registo, a organização, a divulgação, a conservação, o apagamento, ou outros;

**"violação de dados pessoais "**- uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais.

**"subcontratante "**- pessoa singular ou coletiva que trata dados de caráter pessoal por conta do responsável pelo tratamento. Trata-se, portanto, de uma entidade prestadora de um serviço e que em alguma medida intervém no processo de tratamento de dados pessoais (ex: Empresa contratada para a Medicina no Trabalho);

## Sobre as categorias especiais de dados pessoais (exº relativos à saúde e condição física ou psíquica)

Em muitas situações, o IPV está legalmente obrigado a tratar dados de categorias especiais e dados sensíveis, tais como dados relativos à saúde e bem estar dos seus titulares( condição física ou psíquica).

Por vezes é recebida, tratada e transmitida informação relativamente à salvaguarda da saúde e bem-estar de alunos, trabalhadores da Instituição, outros, que pode estar sujeita a um regime de confidencialidade (exº relatórios do médico do IPV ou dos Serviços de Psicologia).

**Assim, algumas das situações incluem, entre outras(finalidade do tratamento)**:

✓ Proteger a saúde e o bem-estar dos trabalhadores/ alunos/outros;

✓ Fornecer assistência apropriada (e, se necessário, médica), bem como tomar as medidas apropriadas em caso de emergência, incidente ou acidente, inclusive divulgando detalhes da condição médica de uma pessoa ou outras informações relevantes e do interesse do próprio indivíduo - por exemplo, para aconselhamento médico, proteção social, salvaguarda e cooperação com a polícia ou serviços sociais, para fins de seguro ou para fornecedores ou organizadores de viagens escolares que precisam ser informados sobre dieta ou necessidades de acompanhamento médico;

✓ Prestar serviços educativos no contexto de quaisquer necessidades educativas específicas de um aluno;

✓ Como parte de qualquer reclamação efetuada interna ou externa, processo disciplinar ou de investigação que envolva esta categoria de dados, por exemplo, se incluir elementos de necessidades específicas, de saúde ou de proteção;

✓ Para fins legais e regulamentares (por exemplo, proteção, saúde e segurança) e para cumprir com suas obrigações legais e deveres de cuidados;

✓ Para investigação, ou ensaios clinicos, etc.

## Meios de recolha da informação

No cumprimento da sua missão, o IPV procede à recolha de dados pessoais, incluindo os de saúde, de diversas formas, entre outras, através de:

✓ Boletins de matrícula e renovação de matrícula;

✓ Outros formulários de dados preenchidos por pais, encarregados de educação e/ou alunos ao longo do ano letivo, docentes, não docentes visitantes, outros.;

✓ Dados recolhidos pelos agentes educativos(docentes) no contexto do processo de ensino e aprendizagem e da participação em atividades escolares e extraescolares (dados enriquecidos);

✓ Receção de dados por transferência interna a partir dos diversos serviços e escolas do IPV

✓ Informações sobre os alunos/trabalhadores/outros de determinados serviços médicos e centros de saúde, assim como das respetivas autoridades locais e organismos da tutela, etc.

## Como são tratados os dados pessoais

A recolha de dados pessoais, incluindo os de saúde, destina-se a finalidades relacionadas principalmente com atividades respeitantes aos alunos, pessoal docente e pessoal não docente. Estes dados são incorporados nos ficheiros e outros suportes da titularidade do IPV.

**Fundamento para a recolha e tratamento de dados pessoais:** O IPV, em cumprimento de **obrigação legal**(exº justificação de faltas por doença ao abrigo da Lei Geral do Trabalho em Funções Públicas e Código do Trabalho)**, execução de contrato ou para diligências pré- contratuais**(exº robustez física para o exercício de funções públicas), de **interesse público(**recolha de dados de saúde pela Direção Geral da Saúde para controlo da COVID**), consentimento do titular dos dados**, **defesa de interesses vitais do titular dos dados ou de outra pessoa singular** (exº para realização de determinado exame médico imprescindível), **interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, (**exº medição da temperatura durante a pandemia), recolhe os dados pessoais, incluindo os de saúde, necessários e adequados para entre outras,

✓ Matrícula e inscrição de alunos

✓ Serviços de psicologia e orientação

✓ Serviços de cantina e bar e informação relativa a restrições alimentares

✓ Ação social escolar

✓ Registo de assiduidade

✓ Proteger a saúde e bem-estar dos alunos/trabalhadores / outros e fornecer assistência adequada

✓ Realizar ou cooperar com qualquer reclama o escolar ou externa, processo disciplinar ou de investigação

✓ Desporto Escolar

✓ Trabalho da Comissão de Ética

✓ Envio de Newsletters e outra Informação

Estes dados poderão estar armazenados em suporte físico ou digital, tais como, nas bases de dados das aplicações de gestão de alunos, SAS, vencimentos, RH, bibliotecas e demais serviços, nos processos individuais físicos, em pastas próprias, e que desejavelmente, deverão assegurar o cumprimento dos deveres de sigilo e confidencialidade, com definição prévia de permissões de administração e de acesso e respetivo registo de acesso, no estrito cumprimento dos deveres inerentes às funções exercidas de quem com eles contacta.

Podem ainda ser recolhidos dados pessoais necessários à interoperabilidade de redes e sistemas informáticos públicos e no âmbito da Administração Pública e com entidades externas (nacionais, europeias ou internacionais)

## Conservação de Dados Pessoais

Todas as operações de tratamento de dados e respetivos registos de atividade, são previamente definidas pelo Responsável do Tratamento de Dados (RT), no caso o IPV.

Os dados pessoais deverão ser conservados por prazos diferentes (mais curtos ou mais alargados), consoante a finalidade a que se destinam tendo em conta critérios legais, bem como a necessidade e a minimização do respetivo tempo de conservação, sem prejuízo dos prazos legalmente definidos para conservação de determinados documentos e dados (por exemplo para arquivo de interesse público ou para investigação)

Os dados pessoais em suporte digital, em regra, estão armazenados em Cloud (por ex: Office365) e/ou em bases de dados das respetivas aplicações de gestão internas, alojadas em servidor dedicado, e que desejavelmente, deverão garantir a sua anonimização e manutenção da capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada, no caso de um incidente físico ou técnico (para o efeito o IPV, terá de ter um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas a fim de garantir a segurança do tratamento e de acordo com políticas de utilizador do domínio da rede interna).

Os dados pessoais em suporte físico, deverão ser conservados em local próprio, com cumprimento das medidas de segurança adequadas e previamente aprovadas pelo Responsável pelo Tratamento de Dados (RT), com garantia da sua confidencialidade.

## Interconexão de Dados

Os dados pessoais, no cumprimento de normativos legais ou na execução de prestação de serviço público educativo, podem ter de ser comunicados, **entre outras**, às seguintes entidades públicas:

Ministério da Tutela

Ministério das Finanças

Ministério da Saúde

Ministério do Trabalho, Solidariedade e Segurança Social

## Deveres

## Constituem deveres do pessoal docente e não docente e outros:

- Respeitar a confidencialidade dos dados pessoais a que têm acesso no exercício das suas funções e após cessação das suas funções, quando for o caso;
- Respeitar as políticas de segurança no uso da rede informática do IPV, utilizando palavras-passe seguras e respeitando o nível de acesso definido, relativo a dados dos alunos e demais elementos do IPV;
- Comunicar à Equipa Responsável pela Segurança e ao Encarregado de Proteção de Dados quaisquer perdas, ataques, dados transmitidos de forma ilícita ou irregular, discriminando que dados, quem foi afetado, e em que contexto para cumprimento das formalidades fixadas no Regulamento Geral de Proteção de Dados;
- Utilizar comunicações cifradas, utilizando apenas correio eletrónico institucional para qualquer comunicação relativa a assuntos do IPV;
- Os acessos remotos à Instituição (por ex: via VPN), apenas podem ser efetuados desde que garantida a privacidade e encriptação de dados e aprovados pelo Responsável pelo Tratamento IPV;
- Evitar em público conversas ou discussões que potencialmente divulguem informações sobre dados pessoais de alunos, trabalhadores ou outros utilizadores;
- Guardar documentação em formatos físicos de forma segura;
- Utilizar exclusivamente o correio eletrónico institucional para comunicações relativas a todos os assuntos de trabalho no IPV, uma vez que este sistema é encriptado e auditável;
- Validar junto do Responsável pelo Tratamento IPV as interconexões de dados;
- Verificar as permissões e consentimentos para retratos, fotografias e recolha de imagens dentro do IPV;
- Na divulgação de atividades, não colocar informações que identifiquem crianças, como nomes, fotos, registos vídeo e áudio.

## Boas Práticas na Transmissão de Dados entre Docentes:

- Usar exclusivamente o endereço de correio eletrónico institucional;
- Evitar pastas partilhadas na rede interna com permissões públicas para armazenar informação relativa a alunos;
- Usar sempre a conta pessoal nos computadores do IPV, terminando sessão após utilização dos mesmos;
- Usar serviços de armazenamento em Cloud (Dropbox, Google Apps...), depois de verificar se garantem privacidade e encriptação de dados;
- Usar pastas partilhadas em serviço de armazenamento em Cloud, depois de se certificar que estas são acessíveis apenas no perfil individual de utilizador;

Encriptar grelhas de registo de avaliação com palavra-passe conhecida apenas pelos elementos responsáveis pela avaliação

## Boas Práticas na Gestão de Dados

- A palavra-passe pessoal e intransmissível, deve ser complexa e constituir-se, por exemplo, por letras maiúsculas, minúsculas, números e símbolos (como “!” ou “*”) Não deve repetir letras ou números, nem sequências alfabéticas, numéricas ou de teclado.
- Nunca, sob qualquer pretexto, devem ser fornecidas palavras-passe a terceiros (quer pessoais de acesso a perfil de utilizador, quer de administração de computador);
- Reforçar cuidados com palavras passe;
- Utilizar autenticação de duplo fator no correio eletrónico institucional, sempre que se justifique ou seja possível;
- O Responsável pelo Tratamento (IPV) aprova uma política de segurança e de acessos à informação.

## Incidentes de CiberSegurança e de Violação de Dados Pessoais ( Ver mais )

Sempre que se verifiquem possíveis incidentes de quebra de confidencialidade, disponibilidade ou integridade, por exemplo, documentos extraviados, acessos indevidos, publicações indevidas, bloqueio de dados por cifragem (ransomware) ou outros, o Responsável pelo Tratamento e o DPO, são informados de imediato para proceder à respetiva análise de risco e consequente tomada das medidas.

Caso se conclua tratar-se de um incidente de CiberSegurança ou de violação de dados pessoais, na qual se verifiquem existência de riscos para os involvidos, deverão as situações serem reportadas ao Centro Nacional de CiberSegurança e à Comissão Nacional de Proteção de Dados.