Regulamento Geral
de Proteção de Dados

eduBOX

Visão geral do RGPD

Direitos das pessoas singulares

Expande significativamente os direitos das pessoas singulares e a informação que tem de ser facultada relativamente às atividades de tratamento.

Privacidade do princípio ao fim

Incorporação das considerações de privacidade em todos os aspetos, podendo apenas ser usados os dados estritamente necessários à finalidade a que se destinam.

Encarregado da proteção de dados

Poderá ser obrigatório. Exige conhecimentos especializados em direito da proteção de dados. Pode ser um funcionário ou um prestador de serviços.

Portabilidade de dados

As pessoas singulares têm agora o direito de circulação, cópia ou transferência dos dados pessoais - até mesmo para uma empresa concorrente.

Coimas

Podem ir até 4% do volume de negócios global anual, ou 20 milhões de euros, o que for mais elevado. A coima poderá ser aplicada mesmo que não haja perda de dados.

Consentimento

Tem de ser confirmado por uma declaração ou outro ato positivo inequívoco. Não se pode presumir o consentimento nem usar opções pré-selecionadas em sites.

Notificação obrigatória de violação de dados

Os responsáveis pelo controlo de dados têm de notificar as autoridades de controlo locais - CNPD, em Portugal - até 72 horas após tomarem conhecimento do facto. Violações graves têm de ser notificadas às pessoas singulares.

Âmbito de aplicabilidade alargado

Abrange a sua empresa e ainda as que fazem tratamento de dados em seu nome — mesmo fora da UE.

10 Medidas para preparar a entrada em vigor do RGPD – Regulamento Geral de Proteção de Dados

1 Informação aos titulares dos dados

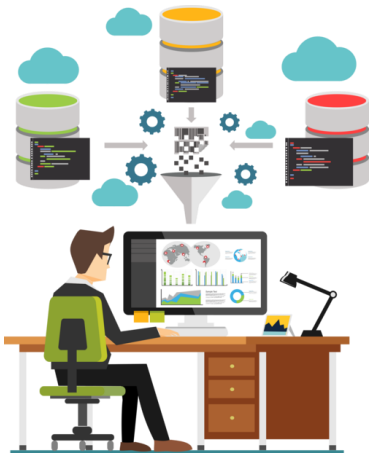
A Empresa / Entidade Pública deve rever a informação que fornece aos titulares dos dados, por escrito ou por telefone, no âmbito da recolha de dados, seja esta realizada diretamente junto do titular ou não.

O regulamento obriga a prestar mais informações do que atualmente, designadamente: a base legal para o tratamento de dados, o prazo de conservação dos dados, informações mais detalhadas sobre as transferências internacionais, a possibilidade de apresentar queixa junto da CNPD. Dentro das exigências de maior transparência, ter em atenção que as informações devem ser prestadas aos cidadãos de forma concisa, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. Deve ser tido particular cuidado quando as informações são dirigidas a crianças.

Assim, vai ser necessário reformular impressos, políticas de privacidade e todos os textos que prestem informação aos titulares dos dados, ao mesmo tempo que deverá verificar se está efetivamente a fornecer, em todas as situações, a informação exigida por lei.

2 Exercício dos direitos dos titulares dos dados

A Empresa / Entidade Pública deve rever os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, atendendo às novas exigências especificas do regulamento neste domínio quanto à tramitação dos pedidos, em especial aos prazos máximos de resposta. Todo o procedimento deve ser devidamente documentado.



A informação contida nesta seção é da autoria da Comissão Nacional de Proteção de Dados (CNPD). Seguindo as diretrizes da CNPD, foi escrito respeitando a integridade do documento original. Como forma de sensibilizar os nossos clientes para se preparem para a entrada em vigor do *General Data Protection Regulation (GDPR)* / Regulamento Geral de Proteção de Dados (RGPD). O documento original pode ser consultado no website da CNPD.

Por outro lado, os direitos dos titulares foram alargados em relação à atual lei, passando a existir o direito à limitação do tratamento e o direito à portabilidade, bem como novos requisitos quanto ao direito à eliminação dos dados e quanto à notificação de terceiros sobre a retificação ou apagamento ou limitação de tratamento solicitados pelos titulares.

Assim, a Empresa / Entidade Pública deve estar preparada para aplicar as novas obrigações, nomeadamente através da manutenção da informação num formato estruturado, de uso corrente e de leitura automática, quando aplicável, e de procedimentos eficazes de comunicação com as entidades terceiras a quem transmitiu os dados, de modo a assegurar o exercício efetivo dos direitos.

Por se tratar de direitos fundamentais dos cidadãos, esta é uma área de intervenção essencial, a qual sofreu várias alterações do ponto de vista procedimental, pelo que requer a maior cautela na sua adaptação às novas disposições legais.

3 Consentimento dos titulares dos dados

A Empresa / Entidade Pública deve verificar a forma e as circunstâncias em que foi obtido o consentimento dos titulares, quando este serve de base legal para o tratamento de dados pessoais. O regulamento alarga o conceito de consentimento e introduz novas condições para a sua obtenção, pelo que é necessário apurar se o consentimento obtido pelo responsável pelo tratamento respeita todas as novas exigências. Se assim não for, é imprescindível obter novo consentimento dos titulares dos dados em conformidade com as disposições do RGPD, sob pena de o tratamento de dados se tornar ilícito por falta de base legal.

Particular atenção deve ser dada ao consentimento dos menores ou dos seus representantes legais, considerando as exigências específicas do regulamento para este efeito.

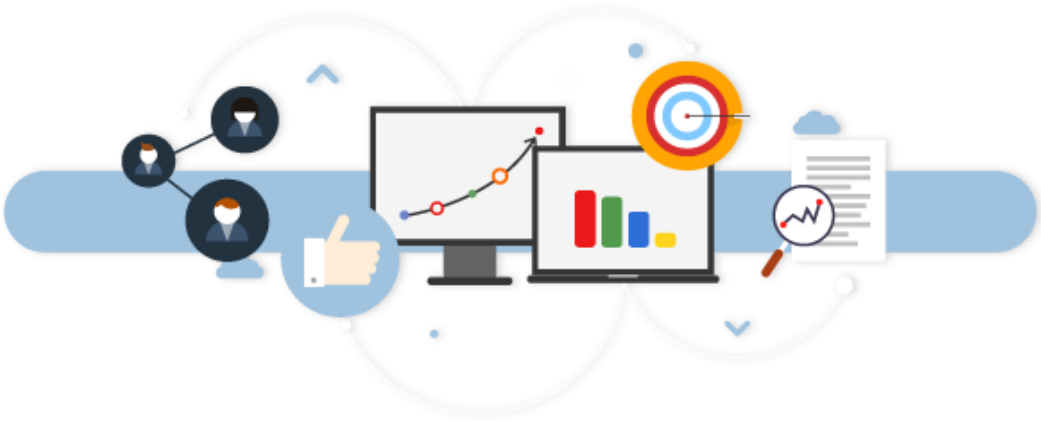
4 Dados sensíveis

A Empresa / Entidade Pública deve avaliar a natureza dos tratamentos de dados efetuados, a fim de apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente se aplicarem condições específicas para o seu tratamento, relativas à licitude do tratamento, aos direitos ou às decisões automatizadas.

O regulamento veio estender o leque das categorias especiais de dados, integrando por exemplo os dados biométricos, que passaram a fazer parte do elenco de dados sensíveis.

Deve analisar também o contexto e a escala destes tratamentos de dados para verificar se daí decorrem obrigações particulares, tais como a designação de um encarregado de proteção de dados.

São considerados dados sensíveis qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável – "titular dos dados". É considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um identificador como o nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, económica, cultural ou social.



5 Documentação e registo de atividades de tratamento

A Empresa / Entidade Pública deve documentar de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação de manter um registo como as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

Uma vez que o regulamento prevê que as entidades em regime de subcontratação, designadas de "subcontratantes", passem a ter quase as mesmas obrigações que os responsáveis pelos tratamentos, estando de igual modo obrigadas a provar que cumprem tudo o que lhes é exigido, a prossecução desta medida de forma atempada é vital, pois terão de começar do zero.

Esta Ação reveste-se de especial relevo no contexto da preparação para a aplicação do novo regulamento, porque permite fazer o levantamento integrado do que está a ser feito, permitindo validar o que é necessário corrigir e adaptar.

6 Contratos de subcontratação

A Empresa / Entidade Pública deve rever os contratos de subcontratação de serviços realizados no âmbito de tratamentos de dados pessoais para verificar se contêm todos os elementos exigidos pelo regulamento.

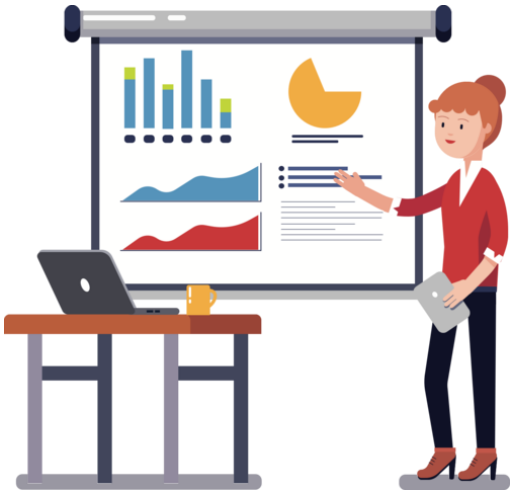
Apesar de se manterem os princípios já vigentes na atual lei de proteção de dados, o RGPD veio especificar o conteúdo dos contratos de subcontratação, impondo a introdução de um vasto conjunto de informações. Assim, será muito provável que os contratos existentes necessitem de ser modificados para respeitar os termos do regulamento. Tal requer algum tempo, se houver várias subcontratações, pelo que é conveniente preparar esta análise.

Quando houver lugar a sub-subcontratação, compete ao subcontratante verificar se detém as autorizações respetivas dos responsáveis pelo tratamento exigidas expressamente pelo novo regulamento; caso contrário, deve obté-las até maio de 2018.

7 Encarregado de Proteção de Dados

A Empresa / Entidade Pública deve preparar a designação do encarregado de proteção de dados com a antecedência devida, até porque este poderá desempenhar um papel fulcral neste período de transição para garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do regulamento. Nesse contexto, especial atenção deve ser concedida à posição do encarregado de proteção de dados dentro da organização e ao reporte direto ao mais alto nível, bem como às funções que lhe são atribuídas pelo RGPD, cujo pleno desempenho requer a satisfação de determinadas condições.

Além das situações previstas no regulamento em que a organização está obrigada a designar um encarregado de proteção de dados, como é o caso das entidades publicas, o responsável pelo tratamento e o subcontratante podem sempre, mesmo não se encontrando no momento em nenhuma das circunstâncias exigíveis, decidir ter um encarregado de proteção de dados na sua organização, pelas evidentes vantagens que tal pode significar para o nível de cumprimento das obrigações.



8 Medidas técnicas e organizativas e segurança do tratamento

A Empresa / Entidade Pública deve rever as políticas e práticas da organização à luz das novas obrigações do regulamento, e adotar as medidas técnicas e organizativas adequadas e necessárias para assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD a partir do momento da sua aplicação.

Essa avaliação, deve ter em conta a natureza, âmbito, contexto e finalidades dos tratamentos de dados, bem como os riscos que deles podem decorrer para os direitos e liberdades dos cidadãos.

Esta apreciação permite ainda tomar as medidas necessárias para confirmar um nível de segurança do tratamento adequado, que garanta designadamente a confidencialidade e a integridade dos dados e que previna a destruição, perda e alterações acidentais ou ilícitas ou, ainda, a divulgação ou acesso não autorizados de dados.

9 Proteção de dados desde a conceção e avaliação de impacto

A Empresa / Entidade Pública deve avaliar rigorosamente o tipo de tratamentos de dados que tenha projetado realizar num futuro próximo, de modo a analisar a sua natureza e contexto e os potenciais riscos que possam comportar para os titulares dos dados, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito.

Embora estes princípios já fossem aplicados no âmbito do princípio da qualidade dos dados, o RGPD vem expressamente prever a sua adoção no momento da definição dos meios de tratamento e no momento do próprio tratamento de dados, pelo que deve ser equacionada a sua aplicação atempada.

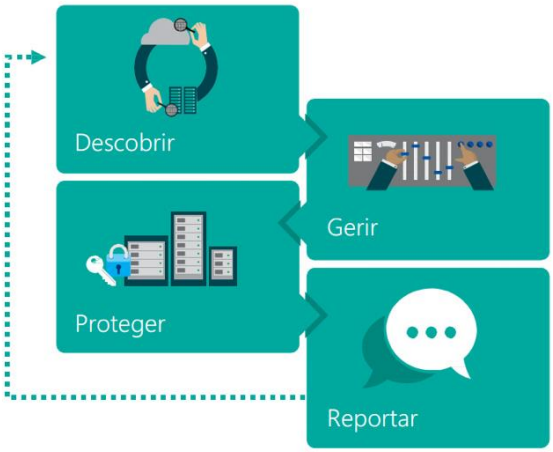
A fim de decidir sobre as medidas mais ajustadas, sejam tendentes à pseudonimização, à minimização dos dados, ao cumprimento dos prazos de conservação da informação ou à acessibilidade dos dados, deve ter em devida conta as características do tratamento e os efeitos que este pode ter nos direitos dos cidadãos; se for suscetível de resultar num elevado risco, deve realizar uma avaliação de impacto sobre a proteção de dados, de modo a adotar as medidas adequadas para mitigar os riscos.

10 Notificação de violações de segurança

A Empresa / Entidade Pública deve adotar procedimentos internos e ao nível da subcontratação, se for o caso, para lidar com casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação entre responsável e subcontratante, envolvimento do encarregado de proteção de dados e notificação à CNPD, atendendo aos prazos prescritos no regulamento.

Nem todas as violações devem ser reportadas à autoridade de controlo, apenas aquelas que sejam suscetíveis de resultar num risco para os direitos dos titulares. Todavia, todas as violações devem ser devidamente documentadas conforme preceituado no regulamento.

Também nalguns casos, em que possa resultar um elevado risco para os titulares, é exigido que estes sejam notificados, pelo que deve ser analisado desde logo o tipo de tratamentos de dados realizados e o potencial risco que pode ocorrer em caso de uma violação de segurança.



Direitos dos Cidadãos

Para além de reforçar os direitos dos cidadãos, o novo regulamento prevê novos direitos e concede-lhes um maior controlo dos seus dados pessoais. Deste modo, o RGPD irá permitir aos cidadãos:

1. Acesso simplificado aos seus dados, incluindo a prestação de mais informações relativamente à forma como os dados são tratados e a garantia de que essas informações são disponibilizadas de forma clara e acessível;
2. Direito à portabilidade dos dados, que irá facilitar a transmissão de dados pessoais entre os prestadores de serviços;
3. Direito à eliminação dos dados. Sempre que um indivíduo não queira mais o tratamento dos seus dados e não existam motivos legítimos para continuar a conservá-los, os dados serão apagados;
4. Direito de ter conhecimentos se os seus dados pessoais foram alvo de pirataria informática. As entidades devem informar prontamente as pessoas das violações graves em matéria de dados.

O RGPD na Edubox

A empresa Edubox S.A. está a avançar com medidas técnicas e organizativas que assegurem e comprovem que o tratamento é realizado em conformidade com o RGPD, incluindo a aplicação de políticas adequadas em matéria de proteção de dados nas aplicações e softwares da empresa.

Todos os dados recolhidos pela Edubox são:

- Objeto de tratamento lícito, leal e transparente em relação ao titular dos dados;
- Recolhidos para finalidades determinadas, explícitas e legítimas;
- Exatos e atualizados sempre que necessário;
- Adequados, pertinentes e limitados ao que é necessário;
- Conservados de forma a que permitam a identificação dos titulares dos dados apenas durante o período necessário;
- Tratados de forma a que garantam a segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidental;
- Tratados apenas se o titular tiver dado o seu consentimento para uma ou mais finalidades específicas.

O cumprimento do código de conduta ou de procedimentos de certificação pode ser utilizado como elemento para demonstrar o cumprimento, garantindo:

- A pseudonimização (quando os campos de identificação contidos num registo de dados são substituídos por um ou mais identificadores artificiais);
- A cifragem (quando os dados são codificados de forma a que apenas possam ser lidos por pessoas autorizadas);
- A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Tendo produtos principalmente *Web Based*, a Edubox S.A. está a preparar-se, a nível dos seus sistemas, com os seguintes procedimentos:

- Cifragem dos dados
  - Passwords dos utilizadores
  - Base de dados
- Navegação por https, colocando uma camada adicional de criptografia utilizando o protocolo TLS. Deste modo, a ligação é encriptada não permitindo o acesso por terceiros

A Edubox tem neste momento na sua estrutura definido o responsável pela área dos dados, designado por EPD (DPO).

Alguns conselhos:

- Revisão/alteração dos Regulamentos (Regulamento de educação) de forma a garantir a recolha de dados das várias fontes (Agrupamentos de Escolas, Juntas de Freguesia ou diretamente aos encarregados de educação):
  - Boletins de inscrição/candidaturas com aceitação dos termos dos regulamentos;
  - Recolher apenas dados relevantes para serviços prestados;
  - Documentar dados recolhidos por titular;
  - Documentar procedimentos que irão utilizar os dados recolhidos.

Na tabela seguinte estão descritos os requisitos gerais e específicos, bem como as regras a ter em conta no Regulamento Geral da Proteção de Dados, apresentado no Conselho de Ministros n.º 41/2018, e feito o paralelismo com o cumprimento destes requisitos e regras pela Edubox S.A.

Requisito Geral		Requisito Específico	Classificação	RGPD na Edubox
As aplicações cliente (exemplo Android, iOS e Web) devem ser desenvolvidas adotando práticas de desenvolvimento seguro.	Front-End	Seguir as boas práticas de desenvolvimento. Exemplo: *Open Web Application Security Project* (OWASP), no que respeita ao desenvolvimento de código seguro e de submissão desse código a testes de segurança.	Obrigatório.	Cumprido. O software desenvolvido pela Edubox respeita as boas práticas e *standards* da indústria.
		Utilização de sessões seguras com protocolo de Segurança.	Obrigatório.	Todos os serviços disponibilizados pela Edubox passaram recentemente a funcionar sobre o protocolo https que aplica encriptação 256 bits em todos os pedidos entre o cliente e o servidor.
		Recomenda -se o uso de *Transport Layer Security* (TLS), na sua versão mais recente.	Recomendado.	As comunicações estão a utilizar TLS 1.2 que é o *standard* neste momento.
		Não guardar informação pessoal no browser, memória ou disco, para além do tempo da sessão e apenas na medida do necessário.	Obrigatório.	Os dados relativos à sessão atual estão encriptados, sendo apagados aquando do seu término. Nenhum destes dados é pessoal.
	Camada Aplicacional	Utilização de sessões seguras com protocolo de Segurança.	Obrigatório.	O acesso a todas as nossas soluções é feito em https.
		Recomenda -se o uso de TLS, na sua versão mais recente, na comunicação com as camadas adjacentes.	Recomendado.	As comunicações estão a utilizar TLS 1.2 que é o standard neste momento.
		Se possível usar certificados através de *Application Programming Interface* (API), não sendo desta forma necessário o uso de palavras-passe.	Recomendado.	As comunicações entre os diferentes módulos aplicacionais são efetuadas com recurso a *tokens* de acesso válidos por períodos de tempo limitados.
		Não é permitida a utilização de credenciais em *plain text*, quer no código quer em ficheiros de configuração.	Recomendado.	Todas as *passwords* necessárias para acesso e comunicação entre camadas encontram-se encriptadas e ofuscadas utilizando as ferramentas mais recentes e indicadas pelos fornecedores.

		Deve ser evitado palavras-passe embebidas no código.	Recomendado.	Não existem *passwords* no código nas soluções disponibilizadas pela Edubox
		As credenciais que necessitem de ser armazenadas em ficheiros de configuração devem estar codificadas (HASH — mínimo SHA 256).	Recomendado.	Em caso de necessidade tecnológica, a encriptação destas credenciais cumpre os requisitos de segurança.
	Camada de Base de Dados	Comunicação com camada aplicacional através de autenticação por certificado válido por período não superior a 2 anos, no caso de as camadas serem físicas ou logicamente distintas.	Obrigatório.	Existe separação das camadas. A comunicação entre as camadas é encriptada e apenas é feita internamente na mesma rede. A camada de dados está protegida por *firewall* e não é possível chegar a estas a partir do exterior ou das aplicações de *frontend*.
		Prever cifra de informação pessoal (recomenda-se mínimo 2048 bit) apenas se a aplicação cliente tiver camada de BD física e logicamente distinta, usando preferencialmente tecnologia que permita interoperabilidade entre sistemas.	Obrigatório.	Os dados armazenados nos nossos sistemas apenas podem ser visualizados por pessoas devidamente autorizadas (trabalhadores), existindo um *log* de operações sobre os mesmos.
Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações.	Front-End	O processo de autenticação deve ser sempre iniciado e mantido em sessão segura.	Obrigatório.	Todas as sessões são mantidas em segurança através do uso de *tokens* encriptados. Estes *tokens* são válidos por um período de tempo limitado e são únicos por cada sessão.
		Recomenda -se: 1) o uso de TLS, na sua versão mais recente; ou 2) o uso de palavra - passe, preferencialmente em combinação com outro fator (*Double Factor Authentication* - 2FA), como por exemplo: Palavra -passe + SMS *Token* Palavra-passe + *smartcard* Palavra-passe + biometria Palavra-passe + padrão gráfico Palavra-passe + cartão de coordenadas Palavra-passe + código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR-*Code*.	Recomendado.	Utilização do protocolo TLS 1.2 em todas as comunicações entre o cliente e o servidor, assegurando que os dados não possam ser capturados em trânsito. Desta forma apenas o cliente e servidor conhecem o conteúdo da comunicação.

		Dados pessoais de sessão excluídos das variáveis *Uniform Resource Locator* (URL) ou de outras variáveis visíveis ao utilizador.	Recomendado.	A autenticação de localizações externas é feita recorrendo a *tokens* de acesso obtidos através de comunicação segura e encriptada com o *backend*. Nenhuma *password*, *login* ou informação pessoal do utilizador são passados via URL (*query strings*).
		Credenciais de início de sessão transmitidos através do seu HASH, mínimo *Secure Hash Algorithm* -256 (SHA -256), ou utilização de cifra ou codificação para a transmissão de dados pessoais (nome do utilizador e palavra -passe em HASH e restantes dados cifrados).	Recomendado.	Os dados de autenticação são encriptados a partir do momento da sua submissão no *frontend* da aplicação.
		Sempre que aplicável, a palavra-passe deve ter no mínimo 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa. A sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório.	Em fase de implementação, na ótica do cliente. Na ótica dos administradores já é cumprida esta regra.
		Recomenda-se que para novos sistemas seja sempre usado como padrão de autenticação o 2FA.	Recomendado.	Não aplicável
	Camada Aplicacional	A palavra-passe dos administradores deve ter no mínimo 13 caracteres e ser complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório.	Cumprido.
		Para todos os administradores deve -se utilizar Padrão de autenticação 2FA. Exemplos: Palavra-passe + *smartcard* Palavra-passe + biometria Palavra-passe + certificado (por exemplo X.509, da ITU -T para ICP, válido por período não superior a 2 anos).	Obrigatório.	Não aplicável.

		Como mecanismo de proteção e segurança da informação recomenda-se o uso de *Token*.	Recomendado.	Para acesso a esta camada, já está implementada a utilização de *tokens*, os quais apenas são válidos por um período de tempo limitado.
		Comunicação com camadas FE ou BD através de sessão segura, com prévia autenticação se camadas forem física ou logicamente distintas.	Obrigatório.	Cumprido.
		Deve ser evitado palavras-passe embebidas no código. Quando tal não for possível, devem estar codificadas (HASH, mínimo SHA -256).	Recomendado.	Cumprido.
		Se possível, usar certificados através de API, não sendo desta forma necessário o uso de palavras-passe.	Recomendado.	Não aplicável.
		Autenticação de elementos comunicantes garantida por validação de informação estática ao nível da rede.Exemplos: 1) utilização de IP fixo + *hostname* + *MacAddress* + fatores de autenticação, ou 2) Utilização de certificados.	Obrigatório.	As camadas de dados são física e logicamente distintas e apenas permitem a comunicação entre os elementos da sua própria rede.
	Camada de Base de Dados	A palavra-passe deve ter no mínimo 13 caracteres e ser complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório.	Cumprido.
		Dados pessoais de autenticação, transmitidos através do seu HASH (mínimo SHA -256), ou recorrendo à cifra ou codificação para efetuar essa transmissão.	Recomendado.	Cumprido. Esta regra utiliza as ferramentas de autenticação aconselhadas pelos fornecedores do *software* e segue os *standards* da indústria.
Atribuição de direitos de acesso e privilégio de forma restrita e controlada.	Front-End	Criação de perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (*Create, Read, Update, Delete* — CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Já existem mecanismos de atribuição de permissões nos sistemas atualmente disponibilizados, no entanto, estes estão atualmente a ser melhorados para dar resposta ao nível do refinamento necessário ao tratamento de

				determinados dados pessoais.
		Criação de registo de acesso, alteração e remoção (*logs*), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório	Já existem mecanismos de registo de operações sobre todos os dados armazenados, no entanto, estamos a fazer um planeamento cuidado para melhorar estes sistemas e possibilitar aos administradores do sistema o acesso direto aos registos destas operações.
	Camada Aplicacional	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Já existem mecanismos de atribuição de permissões nos sistemas atualmente disponibilizados, no entanto estes estão atualmente a ser melhorados para dar resposta ao nível de refinamento necessários ao tratamento de determinados dados pessoais.
		Criação de registo de acesso, alteração e remoção (*logs*) com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.	Já existem mecanismos de registo de operações sobre todos os dados armazenados, no entanto estamos a fazer um planeamento cuidado para melhorar estes sistemas e possibilitar aos administradores do sistema o acesso direto aos registos destas operações.
	Camada de Base de Dados	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Já existem mecanismos de atribuição de permissões nos sistemas atualmente disponibilizados, no entanto, estes estão atualmente a ser melhorados para dar resposta ao nível do refinamento necessário ao tratamento de determinados dados pessoais.
		Criação de registo de acesso, alteração e remoção (*logs*), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.	Já existem mecanismos de registo de operações sobre todos os dados armazenados, no entanto, estamos a fazer um planeamento cuidado para melhorar estes sistemas e possibilitar aos

				administradores do sistema o acesso direto aos registos destas operações.

Atribuição das credenciais de acesso de forma controlada através de um processo formal de gestão do respetivo ciclo de vida.	Front-End	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Cumprido pelos sistemas através da atribuição de perfis por tipo de utilizador.
		Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação. Exemplo: Envio de informação de autenticação por SMS com validade limitada (não superior a 5 minutos), com primeiro acesso a implicar sempre a redefinição da informação enviada; Envio de informação de autenticação gerada automática e aleatoriamente, enviada por Envelope (semelhante ao do envio de dados do Cartão de Cidadão).	Obrigatório.	Os mecanismos de geração de credenciais de acesso cumprem o estipulado neste ponto, no entanto, a forma de veiculação da informação para os seus legítimos destinatários é definida pelos nossos clientes. Este processo é acompanhado e alvo de aconselhamento pelas equipas de implementação da Edubox.
	Camada Aplicacional	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Cumprido pelos sistemas através atribuição de perfis por tipo de utilizador.
		Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório.	Os mecanismos de geração de credenciais de acesso cumprem o estipulado neste ponto, no entanto, a forma de veiculação da informação para os seus legítimos destinatários é definida pelos nossos clientes. Este processo é acompanhado e alvo de aconselhamento pelas equipas de implementação da Edubox.
	Camada de Base de Dados	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Cumprido pelos sistemas através atribuição de perfis por tipo de utilizador.
		Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório.	Os mecanismos de geração de credenciais de acesso cumprem o estipulado neste ponto, no entanto, a forma de veiculação da informação para os seus legítimos destinatários é definida pelos nossos clientes. Este processo é

				acompanhado e alvo de aconselhamento pelas equipas de implementação da Edubox.

Revisão de direitos de acesso de utilizadores em intervalos regulares.	Front-End	Processo de renovação de conta do utilizador de acordo com os mesmos requisitos de segurança da criação do mesmo, não devendo ter um ciclo de vida superior a 180 dias.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Deve ser desativada uma conta de utilizador quando o mesmo não tem atividade sobre a conta durante 3 meses.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
	Camada Aplicacional	Processo de gestão de validade de perfis.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Processo de gestão de validade de perfis automatizado.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório.	Levantamento de requisitos junto dos nossos parceiros por forma a perceber as necessidades e formas de implementação.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.

	Camada de Base de Dados	Processo de gestão de validade de perfis.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Processo de gestão de validade de perfis automatizado.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório.	Levantamento de requisitos junto dos nossos parceiros de forma a perceber as necessidades e formas de implementação.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados.	Front-End	A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta de utilizador é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Ação dos utilizadores sobre dados pessoais (CRUD) deve permitir a sua auditoria em registo de atividade (*logs*).	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
	Camada Aplicacional	Para Administradores de Sistemas, Redes e Aplicacional, caso acedam a dados pessoais, aplicam -se os requisitos da camada FE.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Processo de gestão de validade de contas de utilizadores.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.

		Processo de gestão de validade de contas de utilizadores automatizado.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade limitada.	Obrigatório.	Levantamento de requisitos junto dos nossos parceiros de forma a perceber as necessidades e formas de implementação.
		Recomenda -se: 1) uma periodicidade bimestral; ou 2) quando se verifique uma alteração no mapa de pessoal associado a esta função.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
	Camada de Base de Dados	Para Administradores de Bases de Dados, Administradores de Sistemas, de Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
	Camada de Base de Dados	Processo de gestão de validade das contas dos utilizadores.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
	Camada de Base de Dados	Processo de gestão de validade das contas dos utilizadores automatizado.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
	Camada de Base de Dados	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
Restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil).	Front-End	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.

	Camada Aplicacional	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Já existe um sistema de atribuição de perfis para todos os utilizadores do sistema, no entanto, estamos a trabalhar para melhorar os tipos de dados a que cada utilizador terá acesso, assim como o registo destes acessos.
		Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
	Camada de Base de Dados	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Já existe um sistema de atribuição de perfis para todos os utilizadores do sistema, no entanto, estamos a trabalhar para melhorar os tipos de dados a que cada utilizador terá acesso, assim como o registo destes acessos.
		Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 3.º trimestre de 2018.
Automatização dos processos de concessão, revisão, análise e revogação de acesso.	Aplicam-se as mesmas disposições que em «Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados» e «Revisão de direitos de acesso de utilizadores em intervalos regulares».		Obrigatório.	Em fase de planeamento. Prevê-se a conclusão no final do 4.º trimestre de 2018.
Procedimentos seguros de início de sessão.	Aplicam-se as mesmas disposições referidas em «Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o acesso controlado por um procedimento seguro de início de sessão».		Obrigatório.	Em fase de planeamento.
	Deve ser guardado registo de atividade (*log*) de todas as ações que um utilizador efetue sobre dados pessoais, independentemente do seu perfil e função.		Obrigatório.	Em fase de planeamento.

Capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis.		Todos os registos de atividade (*log*) devem ser armazenados apenas em modo de leitura, devendo, com uma periodicidade máxima de 1 mês, ser englobados num único bloco de registos e assinado digitalmente (garantia de integridade).	Obrigatório.	Em fase de planeamento.
		Deve ser guardado registo de atividade (*log*) de todos os acessos e tentativas falhadas de acesso, obedecendo aos requisitos anteriores.	Obrigatório.	Em fase de planeamento.
		Garantir que os registos de atividade provenientes dos diversos subsistemas (Sistemas Operativos, aplicações, *browsers*, Sistema de Gestão de Base de Dados — SGBD, etc.) são inequivocamente associados à sua origem.	Obrigatório.	Em fase de planeamento.
		Os registos de atividade (*log*) devem conter, no mínimo, o endereço de acesso (IP e Porto), *Host*, HASH da conta do utilizador que efetuou a ação, ação efetuada (CRUD), Tipo de Dado Pessoal onde a ação foi efetuada, data/hora/minuto/ segundo (*TimeStamp*) da ação, alteração efetuada sobre o dado pessoal.	Obrigatório.	Em fase de planeamento.

Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional.		Tendo em vista garantir que a entidade responsável pelo tratamento de dados deve definir e implementar mecanismos de proteção da informação em função da sua relevância e criticidade, deve ser implementado: - Deteção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas nas *firewall*, *Intrusion Detection System* — IDS, etc.); - Extensão desta proteção desejavelmente a todos os dispositivos (incluindo móveis) com acesso a dados pessoais nos sistemas corporativos; - Mecanismo de cifra ponto a ponto sempre que houver necessidade de aceder remotamente ao FE (e apenas a esta camada), como por exemplo com recurso à tecnologia *Virtual Private Network* (VPN).	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.

Proteção dos dados contra modificações não autorizadas, perdas, furtos e divulgação não autorizada.	Front-End	FE desenvolvido e em produção de acordo com as melhores práticas de segurança, garantindo a proteção desta camada aos ataques mais comuns (SQLi, injeção de código, etc.).	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
		FE Recomenda-se as práticas recomendadas em *Open Web Application Security Project* (OWASP).	Recomendado.	Cumprido.

		Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
	Camada Aplicacional	Camada aplicacional segregada da rede ou ambiente com visibilidade e/ou acesso exterior.	Obrigatório.	Cumprido.
		Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
	Camada de Base de Dados	Camada de BD segregada da rede ou ambiente com visibilidade/acesso exterior.	Obrigatório.	Cumprido
		Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
		Mascaramento, anonimização ou, sendo necessário, cifra dos dados pessoais transmitidos ou acedidos.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
		Dados armazenados (incluindo os existentes em volumes de salvaguarda — *backups*) devem ser cifrados e assinados digitalmente.	Recomendado.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
		Recomenda-se que, para dados pessoais considerados muito críticos, o seu armazenamento seja efetuado de forma fragmentada e em locais físicos distintos, mantendo-se, todavia, a sua unicidade e integridade lógica.	Recomendado.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais.		Deve ser garantida a integridade das zonas *Domain Name System* (DNS) onde se encontra inserido o sistema e o ecossistema envolvente, recorrendo às boas práticas de DNSSec e de configuração de sistemas de Correio Eletrónico (por exemplo, *Sender Policy Framework* — SPF, *DomainKeys Identified Mail* — DKIM, *Domain -based Message Authentication*, *Reporting and Conformance* — DMARC, entre outros).	Obrigatório.	Cumprido.

	Deve ser utilizada tecnologia de comunicação segura (por exemplo VPN), com sistema de autenticação forte (preferencialmente através de certificados), para que a transmissão de dados entre entidades de ambientes tecnológicos distintos seja efetuada em segurança.	Recomendado.	Cumprido.

Os sistemas de armazenamento devem garantir redundância e disponibilidade, não devendo existir nenhum «single point of failure».	A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.	Obrigatório.	Cumprido.
	Devem existir dois tipos de *backups* (*online* e *offsite*), que devem obedecer aos mesmos requisitos de segurança definidos para os sistemas produtivos.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
	Os *backups offsite* devem ser guardados numa localização que não esteja exposta aos mesmos riscos exteriores da localização original, podendo ser da organização, mas geograficamente distinta e/ou afastada.	Obrigatório.	A analisar a aplicabilidade deste ponto as soluções disponibilizadas pela Edubox.

As redes e sistemas de informação devem possuir as funcionalidades necessárias ao respeito pelos direitos do titular dos dados.	Os sistemas devem estar capacitados para classificar, priorizar, pesquisar, editar e apagar os dados pessoais.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
	Os sistemas devem possuir os controlos necessários que permitam a identificação, autenticação, acesso e validação dos dados pessoais armazenados.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.

As tecnologias de informação a implementar devem permitir a portabilidade e a exportação de dados pessoais.	Deve -se garantir a utilização de formatos digitais compatíveis, que assegurem a interoperabilidade técnica e semântica dentro da Administração Pública, na interação com o cidadão ou com a empresa e para disponibilização de conteúdos e serviços, adotando as especificações técnicas e formatos digitais definidos no Regulamento Nacional de Interoperabilidade Digital, aprovado pela Resolução do Conselho de Ministros n.º 91/2012, ou noutroque o venha a substituir.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.

Devem ser definidas políticas que garantam a segurança dos dados pessoais, em alinhamento **com a estratégia superiormente definida para a segurança do tratamento de dados pessoais.**	As políticas que garantam a segurança do tratamento de dados pessoais devem abranger: A priorização e classificação dos dados de acordo com os critérios de sensibilidade e criticidade predefinidos; A criação; A modificação; A transmissão; A recolha (independentemente do respetivo meio ou processo); A destruição; O armazenamento (incluindo a retenção); A pesquisa de dados.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.
	Deve -se garantir o conhecimento, a todo o tempo, dos ativos de informação relativamente a dados pessoais, de modo a permitir identificar inequivocamente o estado da informação em todo o seu ciclo de vida.	Obrigatório.	A analisar a aplicabilidade deste ponto relativamente às soluções disponibilizadas pela Edubox.

Poderá consultar mais informações sobre o RGPD:

- Regulamento Geral de Proteção de Dados
- Orientações sobre o direito à portabilidade dos dados / Revisões
- Orientações sobre os encarregados da proteção de dados (EPD) / Revisões
- Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante / Revisão / Anexo com perguntas frequentes
- Orientações relativas à Avaliação do Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (EU) 2016 / 679
- Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679
- Notificação de violação de dados pessoais (EN) / Revisões
- Decisões individuais automatizadas e definições de perfis (EN) / Revisões

Antiga Fábrica de Moagens de Aveiro
Rua Calouste Gulbenkian, Edifício A
Gabinete 31.2.36
3810-074 Aveiro

NIPC: 509 295 967

Telefone: 234 380 316

Telemóvel: 963 946 477

Email: geral@edubox.pt

Website: www.edubox.pt