qualificação PME

Segurança da Informação para PME

Guia Técnico de Segurança da Informação para as Empresas

aevc
ASSOCIAÇÃO EMPRESARIAL DE VIANA DO CASTELO

ÍNDICE

INTRODUÇÃO

Este Guia foi desenvolvido no âmbito do projeto "Qualificação das PME" e nele se pretende estabelecer as diretrizes as melhores práticas para a proteção das informações internas das empresas, bem como informações de terceiros armazenadas internamente nas empresas. Trata-se de um documento que contempla um conjunto de princípios, práticas e cuidados necessários que orientar a gestão das empresas ao nível da segurança das informações das empresas.

A segurança da informação e a proteção de dados pessoais são desafios levantados e exponenciados pela ubiquidade de ferramentas digitais de tratamento, onde a falta de controlo e rastreio deficientes sobre os dados tratados levantou questões de privacidade e controlo de dados por parte dos titulares que identificam ou tornam identificáveis.

Para as empresas, a segurança da informação e a divulgação dos procedimentos e preocupações de segurança quem mantêm com os dados pelos quais são responsáveis aos clientes e público em geral pode constituir-se como uma vantagem concorrencial e competitiva uma vez que ganham a confiança do público e criam uma diferenciação positiva face à concorrência, ao respeitarem e promoverem o respeito deste património jurídico dos seus utilizadores/clientes.

As perdas de dados podem ter consequências para as empresas, nomeadamente a nível da disrupção da atividade comercial da empresa e continuidade do negócio, transtorno de tempo a repor dados perdidos, custos monetários, perda irreversível de informação, coimas e processos, etc.

A informação em geral e os dados relativos a clientes em particular será, em grande proporção, um dos maiores ativos que as empresas têm atualmente ao seu dispor, mesmo que os responsáveis não se apercebam deste valor.

Assim quais são os ativos de informação que as empresas têm?

Os ativos de informação que sua organização mantém variam, mas provavelmente incluem muitos dos tipos a seguir enunciados, sem prejuízo de poderem existir outros:

- Dados pessoais de clientes e colaboradores;
- Informações do cliente em sistemas computacionais remotos (ex.: na nuvem);
- Orçamentos;
- Planos de negócios;
- Recursos Humanos;
- Registos de clientes;
- Propriedade intelectual;
- Jurídico;
- Especificações do produto;
- Planificações financeiras;
- Contratual;
- Fornecedores;
- Arquivos históricos e estatísticos;
- Informações fiscais;
- Termos comerciais;
- Procedimentos operacionais.

Estas informações serão valiosas das mais diferentes maneiras; algumas podem ser essenciais para manter a empresa a funcionar (por exemplo, registos de clientes), algumas podem configurar infrações legais pesadas se forem comprometidas e algumas representar um investimento ao longo de muitos anos (por exemplo, a propriedade intelectual).

O regulamento de proteção de dados veio responsabilizar as organizações relativamente aos dados pessoais por elas mantidos e reforçar os direitos dos titulares dos dados, legitimando a respetiva utilização e partilha, para além de ter uniformizado a regulamentação dos dados pessoais no Espaço Económico Europeu.

Os requisitos processuais e de segurança do novo regulamento de proteção dados pessoais exige e implica as empresas na alteração de normas e procedimentos internos de forma que a privacidade dos dados pessoais por elas detidos tenham garantia de confidencialidade, integridade, disponibilidade, autenticidade.

CAPÍTULO I

SEGURANÇA DA INFORMAÇÃO

Da mesma forma que os nossos dados e informações são valiosos para nós, podem também ser para os outros.
O Regulamento Geral de Proteção de dados vem exigir uma atenção cuidada para quem lida com dados pessoais obrigando à implementação de práticas de segurança da informação para salvaguardar a confidencialidade, a integridade, a disponibilidade e a autenticidade da informação.
A segurança da informação requer controlos e provisões sobre proteção de dados. As organizações poderão adotar vários controlos para a segurança da informação, como as normas ISO 27001 e ISO 27002. Se a organização já possuir um sistema de gestão de segurança de informação ou de gestão de qualidade, é provável que já estejam implementados muitos dos controlos exigidos pelo RGPD.

A implantação das normas e procedimentos de segurança têm como objetivo primordial responder às perguntas.

O QUE ACONTECERIA SE ...
… outra pessoa obteve acesso aos nossos dados?
- **Perda de confidencialidade**;

… os nossos dados fossem corrompidos de alguma forma
- **Perda de integridade**;

… Não conseguíamos aceder aos nossos dados?
- **Perda de disponibilidade.**

Se os dados fossem roubados ou perdesse acesso aos mesmos, de que modo é que a organização seria afetada? E se os seus clientes, os funcionários, a sua reputação, as suas finanças, o cumprimento da legislação e obrigações contratuais, a saúde e segurança?

Para a maioria das empresas, a consequência da perda de dados tem consequências graves e podem ameaçar a própria existência da empresa e que podem ser de três tipos:
- Danos físicos;
- Materiais;
- Não materiais.

A organização deverá desenvolver uma metodologia consistente para a gestão do risco, decorrente do tratamento de dados e implementar medidas técnicas e organizativas para assegurar a disponibilidade, integridade e proteção de dados pessoais.

A segurança da informação exige um esforço de toda a organização:

- COMPROMISSO DE GESTÃO – exige o comprometimento da administração ou gerência;

- CRIAÇÃO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – é necessário definir e dar a conhecer regras segurança da informação;

- AVALIAÇÃO DOS RISCOS – é necessário analisar os processos, avaliar os riscos e identificar as lacunas;

- SENSIBILIZAÇÃO E RECURSOS – Evidenciando o compromisso da administração ou gerência, esta deve proporcionar formação e recursos para a implementação;

- MONITORIZAÇÃO, ANÁLISE E MELHORAMENTO - Deve ser implementado um sistema de controle regular de forma a avaliar a eficácia e a detetar fragilidades.

1.1. Incidentes de Segurança

Um incidente de segurança pode ser uma violação real ou potencial de perda de dados. Os utilizadores devem estar sensibilizados para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança ou as chefias.
Mal seja tomado conhecimento de que as informações foram comprometidas de alguma forma, devem ser iniciados os procedimentos definidos para situações em que há violação de dados.

Em determinadas situações, pode ser necessário tratar a área como cena de crime e as evidências devem ser preservadas sempre que possível.
No caso de comprometimento de dados pessoais deverá ser notificada a autoridade de controlo.

1.1.1. Tipo de incidentes que podem acontecer

Os incidentes de segurança podem ser classificados em dois tipos:

a) Acidentais:

- Forças da natureza (i.e., inundações, tempestades, terramotos, etc.);
- Falhas da tecnologia por exemplo (i.e., hardware, software, energia, etc.);
- Fator humano (erros ou omissões).

b) Intencionais ou deliberadas:

- Espionagem;
- Crimes (i.e., roubo, fraude, etc.);
- Intrusões;
- Interceções;
- Vandalismo;
- Terrorismo;
- Funcionários insatisfeitos e desonestos (insiders);
- Outros.

1.1.2. Consequências da violação de dados pessoais

- Perda de controle sobre os dados pessoais;
- Limitação de direitos;
- Discriminação;
- Roubo de identidade ou fraude;
- Perda financeira;
- Reversão não autorizada de pseudonimização;
- Danos à reputação;
- Perda de confidencialidade de dados pessoais.

1.1.3. Circunstâncias que influem na gravidade e na probabilidade

Há determinadas circunstâncias que influem na gravidade e na probabilidade do risco do incidente de segurança:

- O tipo de violação;
- A natureza e a sensibilidade dos dados pessoais;
- Volume de dados.

Vejamos alguns exemplos:

- Uma violação de confidencialidade que provoca a divulgação de informação médica a entidades não autorizadas tem consequências diferentes se a mesma informação fosse destruída;

- Um incidente de segurança relacionado com detalhes do cartão de crédito é naturalmente diferente se os dados que estiverem em causa forem o nome ou número de telefone de um titular;

- Uma combinação de dados pessoais é mais sensível do que uma única informação pessoal: Uma lista de clientes que aceitam entregas regulares pode não ser particularmente sensível, mas os mesmos dados sobre os clientes que solicitaram que suas entregas sejam interrompidas durante as férias sejam informações úteis aos criminosos;

- Não conseguir restaurar o acesso aos dados, por exemplo, a partir de um *backup*, isso é considerado como uma negação permanente de disponibilidade, no entanto se houver uma interrupção significativa do serviço normal de uma organização, por exemplo, provocado por uma falha de energia, os dados pessoais estão apenas temporariamente indisponíveis;

- No contexto de um hospital, se os dados médicos críticos sobre os pacientes não estiverem disponíveis, mesmo temporariamente, isso poderá implicar o cancelamento dos atos médicos representando um risco para os direitos e liberdades dos indivíduos;

- Por outro lado, no caso dos sistemas de uma empresa de distribuição de publicidade não estarem disponíveis por várias horas (por exemplo, devido a uma interrupção de energia), e se essa empresa estiver impedida de enviar email marketing para os clientes, é improvável que este represente um risco para os direitos e liberdades dos indivíduos.

As medidas de segurança e proteção dos tratamentos e respetivos dados devem ser proporcionais à natureza dos mesmos, prevenindo o seu acesso e divulgação não autorizada, modificação e eliminação.

1.2. Política de segurança

É necessário que a organização crie uma política de segurança que define os direitos e as responsabilidades de cada um em relação à proteção dos recursos que utiliza, bem como dos comportamentos do dia-a-dia.

Os utilizadores devem estar familiarizados com as políticas de segurança. Estas devem estar disponíveis e poderem ser facilmente acedidas pelos utilizadores. A sua redação deve ser clara e simples de forma a ser compreendida sem deixar dúvidas.

As políticas de segurança devem ser revistas regularmente ou sempre que se justifique.

As medidas definidas devem incentivar, sempre que possível, o recurso a métodos como a pseudonimização, anonimização e encriptação.

De forma a garantir segurança da informação, é essencial que todos cumpram as políticas definidas, sigam os procedimentos e fiquem atentos a situações suspeitas.

O cumprimento da política de segurança não é opcional.

A política de segurança deverá conter entre outras, e se aplicável, políticas específicas como:

- **Política de senhas**: define as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca;
- **Política de *backup***: define as regras sobre a realização de cópias de segurança, como tipo de media utilizada, período de retenção e frequência de execução;
- **Política de confidencialidade**: define como são tratadas as informações institucionais, ou seja, se elas podem ser repassadas a terceiros;
- **Política de utilização de equipamentos** - define as regras de uso dos recursos informáticos, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas;

- **Política de utilização de emails** - define as regras de utilização dos emails, e as situações que são consideradas abusivas;

- **Política de utilização de dispositivos móveis** e outros equipamentos dentro e fora das instalações;

- **Política de utilização de dispositivos pessoais** (*Bring Your Own Device -BYOD*) - gere as regras para a utilização de equipamentos pessoais e o acesso aos dados pelos quais a organização é responsável.

1.3. Práticas de segurança

1.3.1. Segurança física

Apesar de cada vez mais a informação ser digital, a segurança física ainda desempenha um grande papel na proteção das informações. Podem-se fazer grandes investimentos em ferramentas digitais para impedir o acesso aos meios digitais, mas se permitirmos que pessoas desconhecidas entrem nas nossas instalações ou se deixarmos informações acessíveis a outros, grande parte desse investimento será desperdiçado:

- Segurança de portas e janelas - para impedir a entrada de pessoas estranhas à organização;
- Tenha atenção aos cartões de acesso e *PIN's*;
- Deixe a educação de lado e esteja preparado para desafiar (educadamente) qualquer pessoa que não reconheça, especialmente em áreas seguras;
- Guarde todas as pastas com dados pessoais em armários com portas fechadas à chave, ou seja, em local seguro e de acesso condicionado;
- Não deixe documentos confidenciais à vista: ...em cima da secretária, na impressora ou no *scanner*. Tal como os ficheiros digitais, devem ser guardados e armazenados em sítios de acesso restrito;
- Não utilize o verso de fotocópias com dados pessoais como folhas de rascunho;
- Não forneça qualquer informação com dados pessoais pelo telefone, a menos que seja possível certificar a identidade da pessoa que solicita a informação;

- No caso em que o acesso a determinadas áreas é feito com portas fechadas à chave, estas devem ficar à guarda de um responsável que manterá um registo de pedidos da chave;
- Deverão existir destruidores de papel e de *CD/DVD*.

1.3.2. Acessos e senhas

- As credenciais de autenticação (utilizador/palavra-passe) devem ser únicas e intransmissíveis;
- Não grave as senhas de acesso de forma automática nos sistemas e nos navegadores;
- Não utilize as mesmas senhas de acesso para os sistemas da organização e sistemas pessoais;
- Mantenha as senhas de acesso confidenciais;
- Memorize as senhas de acesso, não devendo ser escritas em papéis ou locais visíveis;
- Mude as senhas de acesso regularmente, mesmo nos sistemas que não o obriguem a fazê-lo;
- Escolha uma senha de acesso forte. A palavra-passe deve ter no mínimo 9 caracteres e ser complexa, significando que 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 (~! @ # $ % ^ & * () _ + | `- = \ {} []:"; '<>?,. /). Em alternativa, a palavra-passe poderá ser constituída por frases ou excertos de texto longo, sem caracter de "espaço";
- Use a autenticação de dois fatores sempre que possível;
- Os acessos aos sistemas e funcionalidades deve ser segmentado em privilégios de acesso diferenciados, com base no princípio da necessidade de conhecer, isto é, cada utilizador deve possuir somente os privilégios necessários para realizar a sua função na organização;
- Deve criar-se e manter atualizada uma lista dos utilizadores e indicação dos respetivos privilégios;
- Para situações específicas de ausências prolongadas como por exemplo licenças, férias, baixas prolongadas, mudança de funções, devem ser definidos procedimentos e regras para a substituição.

1.3.3. Segurança de computadores

- Os softwares, nomeadamente os antivírus e o *software anti-spam* devem ser licenciados e mantidos atualizados;
- Os programas não utilizados devem ser eliminados;
- As versões antigas de um programa devem ser eliminadas e mantidas apenas a versão mais recente;
- Faça regularmente *backup* dos dados;
- Bloqueie o computador sempre que há ausências, utilizando a combinação das teclas (Windows + L) e desbloqueado com password;
- Não tire "*screenshots*" ou fotografias quando há dados pessoais ou sensíveis no ecrã;
- Não guarde dados sensíveis localmente no computador;
- No final de cada período de trabalho do utilizador, a respetiva sessão deve ser encerrada;
- Deve ser previsto o encerramento automático da sessão de trabalho do utilizador em caso de inatividade;
- As portas *USB* que não são necessárias devem ser bloqueadas;
- Tenha em atenção a escolha do serviço de assistência aos equipamentos.

1.3.4. Utilização do computador em locais públicos

Quando utilizar o seu computador pessoal em locais públicos:

- Procure manter a segurança física do seu computador, utilizando meios que dificultem o acesso imediato como por exemplo cadeados;
- Configure o computador para solicitar senha ao iniciar e sempre que está inativo por determinado tempo;
- Utilize a encriptação de disco para que, em caso de perda ou furto, seus dados não sejam acedidos.

Ao utilizar computadores de terceiros:

- Opte por navegar anonimamente para garantir sua privacidade;
- Utilize um *anti-malware* online para verificar se o computador está infetado;
- Não efetue transações bancárias ou comerciais;
- Não utilize opções como "Lembrar-me" e "Continuar ligado";
- Não permita que as senhas sejam memorizadas pelo navegador;
- Limpe os dados pessoais guardados pelo navegador, como histórico de navegação e *cookies*;

- Assegure-se de que encerra a sessão da conta de utilizador (*logout*) nos sites que visitou;
- Seja cuidadoso ao ligar dispositivos móveis como *pens*;
- Ao voltar a utilizar o seu computador, altere as senhas de acesso que, por ventura, tenha utilizado.

1.3.5. Dispositivos móveis

- Se disponível, instale um programa *antimalware* antes de instalar qualquer tipo de aplicação, principalmente desenvolvidas por terceiros;
- Mantenha o sistema operacional e as aplicações sempre com a versão mais recente e atualizadas;
- Tenha precaução ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e *plug-ins*. Procure usar aplicações de fontes confiáveis e que tenham uma boa avaliação. Verifique comentários de outros utilizadores.
- Seja cuidadoso ao utilizar os aplicativos de redes sociais, principalmente os baseados em geolocalização, pois pode comprometer a sua privacidade;
- Seja cuidadoso ao usar redes *WiFi* públicas;
- Mantenha os interfaces de comunicação, como *bluetooth*, infravermelho e *WiFi*, desativados e ative-os apenas quando for necessário;
- Configure a ligação *bluetooth* para que o dispositivo não seja identificado (ou "descoberto") por outros dispositivos.

Proteja os equipamentos móveis e os dados nele guardados com medidas de segurança extra:

- Mantenha as informações sensíveis sempre encriptadas;
- Faça *backups* periódicos;
- Mantenha o controle físico sobre os dispositivos móveis, principalmente em locais de risco (evite deixá-los sobre as mesas e tenha cuidado com os bolsos e carteiras quando estiver em ambientes públicos);
- Utilize uma ligação segura sempre que a comunicação envolver dados confidenciais;
- Crie senhas de acesso que sejam complexas (alfanuméricas);
- Configure os equipamentos para que possam ser localizados e bloqueados remotamente, por meio de serviços de geolocalização (pode ser bastante útil em casos de perda ou furto);

- Configure os dispositivos, se possível, para que os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso (use esta opção com bastante cautela).

Ao desfazer-se do seu dispositivo móvel:

- Apague todas as informações nele contidas;
- Restaure a opções de fábrica.

O que fazer em caso de perda ou furto:

- Informe a operadora e solicite o bloqueio do número;
- Altere as senhas que possam estar memorizadas no equipamento furtado (por exemplo, as de acesso ao seu *e-mail* ou rede social);
- Bloqueie os cartões de crédito cujo número esteja memorizado no equipamento furtado.

1.3.6. Media removíveis

Tal como os dispositivos móveis, os media removíveis, como pens USB, cartões de memória e DVDs, podem ser facilmente perdidos ou roubados; Estes tipos de media não devem ser utilizados para guardar informações da empresa.

Nos casos em que se opta por este tipo de dispositivo, a informação deverá ser encriptada e os procedimentos definidos na política de segurança.

Não devem ser usadas *pens USB* que não tenham sido autorizadas pela empresa, pois ao utilizar uma *pen* encontrada por exemplo na rua, pode ser uma forma de introduzir um vírus no computador e no sistema.

1.3.7. Utilização da internet

- Evite a publicação de informações e fotos do local de trabalho nas redes sociais porque podem fornecer, involuntariamente, a estranhas informações úteis para atacar o sistema e a organização, quer seja por meios técnicos ou por engenharia social;
- Não desative o software de firewall;
- Certifique-se de que o navegador e programas associados estão atualizados;
- Verifique a autenticidade das hiperligações;
- Verifique se há HTTPS e o símbolo do cadeado ao realizar transações confidenciais;
- Não descarregue programas desconhecidos;
- Não visite sites suspeitos;
- Seja cuidadoso ao aceitar a utilização de *cookies*;

- Para aceder aos sites de instituições bancárias, digite o endereço diretamente no navegador *Web*. Nunca aceda através do motor de pesquisa ou de uma hiperligação existente numa página ou numa mensagem;
- Ignore mensagens de instituições bancárias com as quais não tenha relação, principalmente aquelas que solicitem dados pessoais ou a instalação de módulos de segurança;
- Sempre que tiver dúvidas, entre em contato com o serviço de apoio ou diretamente com o gerente de conta;
- Não efetue transações bancárias em computadores de terceiros;
- Evite a utilização de redes *WiFi* públicas.

1.3.8. Email

- O email é uma ferramenta que deve ser usada com muito cuidado. Considere o *e-mail* uma forma insegura de comunicar e proceda sempre nesse pressuposto;
- No entanto, também é uma das maneiras mais fáceis de enviar acidentalmente informações para as pessoas erradas. Verifique sempre o destinatário do email antes de carregar no botão enviar;
- Sempre que necessitar de enviar informações confidenciais por *e-mail*, utilize a encriptação e envie a senha de acesso ao destinatário por outro canal.

Ao aceder ao *Webmails*:

- Seja cuidadoso ao aceder a página de seu *Webmail* para não ser vítima de *phishing*. Digite o URL diretamente no navegador e tenha cuidado ao clicar em hiperligações recebidas através de mensagens eletrónicas e nunca utilize um *site* de pesquisa para aceder ao *Webmail* ;
- Evite aceder ao *Webmail* em computadores de terceiros e, caso seja realmente necessário, ative o modo de navegação anónima;
- Certifique-se de utilizar conexões seguras sempre que aceder ao seu *Webmail*, especialmente ao usar redes *WiFi* públicas. Se possível configure para que, por padrão, sempre seja utilizada conexão via "https".

1.3.9. Emails de phishing

O email é provavelmente a forma mais comum de pessoas mal intencionadas nos conseguirem atingir. Um *e-mail* de *phishing* é um *e-mail* que finge vir de um amigo, colega, organização, etc. e geralmente pede que execute alguma ação. Essa ação geralmente pode ser clicar numa hiperligação, abrir um anexo ou ir para um site específico.

Ao fazer isso, estará a permitir a instalação de programas maliciosos no computador sem se aperceber. Como consequência poderá ficar com o conteúdo do disco encriptado, permitir a pesquisa de senhas, tornar-se um ponto de entrada para a rede da organização.

Como perceber um email de *phishing*?

- Normalmente estão mal escritos e com erros de ortografia, no entanto é cada vez menos frequente hoje em dia;
- Geralmente, não são de resposta a um *e-mail* que enviou (embora possam parecer que são de alguém que conhece e que lhe está a enviar o email);
- Se contiverem um anexo como PDF ou Zip anexados que, quando abertos, executam um programa. Uma técnica é passar o rato sobre a hiperligação, SEM CLICAR para ver identificar o destino que normalmente é diferente do indicado;
- Se não tiver certeza acerca da autenticidade de um *e-mail*, entre em contacto o remetente por exemplo, por telefone para verificar se realmente o enviaram.

1.3.10. Utilização de serviços em nuvem

- O armazenamento de dados na nuvem representa, potencialmente, um risco aumentado se não for gerido adequadamente;
- Os centros de dados devem ficar alojados em instalações com as condições de segurança adequadas à proteção dos dados pessoais e serviços contratados;
- Deve-se, também, constituir requisito obrigatório o prestador de serviço possuir servidores físicos dentro do território nacional e/ou da União Europeia;
- Devem ser selecionados prestadores de serviço acreditados e que demonstrem a conformidade com o RGPD.

1.3.11. Cookies

Os Cookies são pequenos arquivos que são guardados no seu computador quando acede a *sites* na Internet e que são reenviados a estes mesmos *sites* quando novamente visitados. São usados para manter informações sobre o utilizador, como carrinho de compras, lista de produtos e preferências de navegação.

Um *cookie* pode ser temporário (de sessão), quando é apagado no momento em que o navegador *Web* ou o programa leitor de *e-mail* é fechado, ou permanente (persistente), quando fica gravado no computador até expirar ou ser apagado. Também pode ser primário (*first-party*), quando definido pelo domínio do *site* visitado, ou de terceiros (*third-party*), quando pertencente a outro domínio (geralmente relacionado a anúncios ou imagens incorporadas à página que está sendo visitada).

Alguns dos riscos relacionados da utilização de *cookies* são:

- **Partilha de informações:** as informações recolhidas pelos *cookies* podem ser indevidamente partilhadas com outros *sites* e afetar a sua privacidade. Não é incomum, por exemplo, aceder pela primeira vez um *site* de música e observar que as ofertas de CD's para o seu género musical preferido já estão disponíveis, sem que tenha feito qualquer tipo de escolha;

- **Exploração de vulnerabilidades:** ao aceder a uma página *Web*, o navegador disponibiliza uma série de informações sobre o computador, como *hardware*, sistema operacional e programas instalados. Os *cookies* podem ser utilizados para manter referências contendo estas informações e usá-las para explorar possíveis vulnerabilidades no seu computador;

- **Autenticação automática:** ao usar opções como "Lembrar-me " e "Continuar ligado" nos *sites* visitados, informações sobre a conta de utilizador são gravadas em *cookies* e usadas em autenticações futuras. Esta prática pode ser arriscada quando usada em computadores infetados ou de terceiros, pois os *cookies* podem ser recolhidos e permitirem que outras pessoas se autentiquem;

- **Recolha de informações pessoais:** os dados preenchidos num formulário *Web* também podem ser gravados em *cookies*, recolhidos por atacantes ou códigos maliciosos e indevidamente acedidos, caso não estejam encriptados;

- **Recolha de hábitos de navegação:** ao aceder a diferentes *sites* onde são usados *cookies* de terceiros, pertencentes a uma mesma empresa de publicidade, é possível a esta empresa determinar seus hábitos de navegação e, assim, comprometer a sua privacidade.

Prevenção:
Não é aconselhável bloquear totalmente os *cookies*, pois poderá impedir a navegação ou o acesso a determinados sites e serviços.

Para prevenir riscos, mas sem comprometer a sua navegação, há algumas dicas que podem ser usadas:

- Configure o navegador para que os *cookies* sejam apagados assim que aquele for fechado;
- Configure o navegador para não aceitar *cookies* de terceiros (ao fazer isto, a navegação não deverá ser prejudicada, pois apenas os conteúdos relacionados as publicidades serão bloqueadas);
- Utilize a opção de navegar anonimamente, quando usar computadores de terceiros (ao fazer isto, informações sobre a sua navegação, incluindo *cookies*, não serão gravadas).

1.3.12. Redes Sociais

- Considere as redes sociais como se estivesse num local público em que tudo o que divulga pode ser lido e acedido por qualquer pessoa tanto agora como no futuro;
- Pense bem antes de divulgar algo, pois não há possibilidade de arrependimento. Uma frase ou imagem fora de contexto pode ser mal-interpretada e causar mal-entendidos. Após uma informação ou imagem propagar-se, dificilmente poderá ser totalmente eliminada;
- Use as opções de privacidade disponíveis nos sites e procure ser o mais restritivo possível;

- Restrinja quem tem acesso ao seu endereço de *e-mail*, pois muitos *spammers* utilizam esses dados para alimentar listas de envio de spam;

- Seja cuidadoso ao associar-se a comunidades e grupos, pois através deles muitas vezes é possível deduzir informações pessoais, como hábitos, rotina e classe social;

- Desconfie de mensagens recebidas mesmo que tenham vindo de pessoas conhecidas, pois podem ter sido enviadas de perfis falsos;

- Ative, quando disponível, as notificações de login, pois assim é mais fácil perceber se terceiros estão a utilizar o seu perfil;

- Use sempre a opção de *logout* para não deixar a sessão aberta;

- Tenha atenção à sua imagem profissional. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode prejudicar de alguma forma;

- Preserve a imagem da empresa. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode prejudicar a imagem e os negócios da empresa;

- Use as redes sociais com perfis distintos para fins específicos. Pode utilizar, por exemplo, uma rede social para amigos e outra para assuntos profissionais.

CAPÍTULO II

O RGPD

O Regulamento do Parlamento Europeu de 27 de abril de 2016 foi criado atendendo às preocupações da União Europeia para proteger os dados pessoais dos europeus.

Com um período de adaptação de 2 anos que durou até 25/05/2018 tem, desde esta data, aplicação direta a todas as entidades que tratem dados pessoais.

O Regulamento aplica-se a todas as empresas que tratem dados pessoais; i.e., que realizem operações com dados de pessoas singulares. As alterações afetam também as empresas que façam negócios com cidadãos da UE, mesmo que sediados fora da EU, ou dados pessoais de pessoas que sejam tratados no EEE – Espaço Económico Europeu.

Umas das novidades introduzidas pelo Regulamento é inversão do ónus da prova, cabendo à organização provar que tem implementadas medidas organizativas e técnicas de proteção aos dados pessoais e dos tratamentos que faz com eles.

O Regulamento exige cuidados às organizações que lidam com dados pessoais obrigando-as a repensar a forma com abordas a segurança e formas de implementação da mesma e a incorporar, por defeito, a segurança da informação na planificação e nas operações quotidianas.

Internamente as empresas necessitam de alterar normas e procedimentos de forma a alcançar o nível de proteção exigido.

2.1. Conceitos introduzidos pelo RGPD

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 apresenta novos conceitos que importa destacar:

2.1.1. Titulares dos dados pessoais

Um dos alicerces da segurança de dados pessoais é a categorização e inventariação das categorias de titulares de dados pessoais tratados pela organização. Sugerimos assim algumas categorias de dados, não se excluindo outras categorias que eventualmente existam em determinados contextos organizacionais:

Trabalhadores;
Colaboradores;
Candidatos a emprego;
Prestadores de serviços;
Utentes;
Clientes;
Público em geral;
Etc...

2.1.2. Responsável de tratamento

Pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro. O responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

2.1.3. Dados pessoais

São constituídos por informação relativa a uma pessoa singular IDENTIFICADA ou IDENTIFICÁVEL («titular dos dados»). É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização,

identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

NÃO são dados pessoais:

- Nº de registo de uma empresa;
- *E-mail* do tipo: info@institutopublico.pt;
- Dados anonimizados.

2.1.4. Tratamento de dados

Operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação e o seu apagamento ou destruição.

2.1.5. Dados especiais

Dados pessoais que, pela sua natureza especialmente sensível, apresentam riscos significativos para os direitos e liberdades fundamentais do titular de dados e por isso merecem proteção específica.
Estes dados não podem ser objeto de tratamento a não ser nos casos excecionalmente previstos no Regulamento, de que são exemplos:

- A origem racial ou étnica;
- As opiniões políticas;
- As convicções religiosas ou filosóficas;
- A filiação sindical;
- Os dados genéticos;
- Os dados biométricos que permitam identificar uma pessoa de forma inequívoca (por exemplo, impressões digitais ou imagens faciais);
- Os dados relativos à saúde (por exemplo, dados relativos a consultas médicas ou baixas médicas);
- Os dados relativos à orientação sexual.

Apenas em determinadas condições as organizações podem efetuar o tratamento de dados sensíveis, como:

- O titular dos dados deu o seu consentimento positivo e explícito;
- O tratamento é necessário para o cumprimento de obrigações legais, por exemplo, em matéria de legislação laboral, de segurança social e de proteção social;
- Quando estão em causa os interesses vitais do titular dos dados;
- Tratar-se de uma fundação, associação ou outro organismo sem fins lucrativos que prossegue fins políticos, filosóficos, religiosos ou sindicais;
- Os dados pessoais foram manifestamente tornados públicos pelo titular dos dados;
- Os dados são necessários para a declaração, o exercício ou a defesa de um direito num processo judicial.

2.1.6. Subcontratante

É qualquer "pessoa, singular ou coletiva, autoridade pública, agência ou outro organismo que trata os dados pessoais por conta do responsável pelo tratamento destes.

São exemplos de subcontratantes:

- Uma empresa que procede ao processamento de salários;
- Uma agência de publicidade que, em nome de um cliente, faz marketing direto junto de consumidores finais;
- Uma empresa de serviços de alojamento de dados web;
- Uma empresa de recrutamento.

2.1.7. Terceiro

Pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais.

2.1.8. Destinatário

Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de

inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento.

2.2. Princípios

O Regulamento estabelece um conjunto de princípios que devem ser aplicados aos tratamentos que forem classificados como necessários. Estes princípios são a corporização do respeito pela informação pessoal enquanto património do seu titular. Apresentam-se de seguida os princípios que deverão estar subjacentes à realização de tratamentos sobre dados pessoais.

2.2.1. Minimização dos dados

Os dados pessoais recolhidos devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados. Não deverão ser recolhidos ou tratados dados que não sejam necessários às finalidades de tratamento.

2.2.2. Exatidão

Os dados devem ser exatos e atualizados sempre que necessário. Os dados que se revelem inexatos devem ser apagados ou retificados sem demora junto dos respetivos titulares.

2.2.3. Limitação das finalidades

Os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais.

2.2.4. Lealdade

Refere-se à aplicação e ao respeito das regras de RGPD e cumprimento de todos os deveres de informação ao Titular de Dados.

2.2.5. Limitação da conservação

A conservação de dados tem que ser feita de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário

para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados.

2.2.6. Transparência

A informação para os titulares de dados deverá ser transparente, em linguagem clara e concisa em todas as fases do tratamento. Os requisitos de transparência no RGPD são aplicáveis independentemente do fundamento jurídico do tratamento. Estas informações devem diferenciar-se claramente de outras informações não relacionadas com a confidencialidade, tais como disposições contratuais ou condições gerais de utilização.

2.2.7. Integridade e confidencialidade

Os dados são tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

2.2.8. Responsabilidade

O responsável pelo tratamento deve a qualquer momento poder demonstrar as evidências do cumprimento com RGPD.

2.3. Licitude do tratamento

Este princípio de tratamento é configurado pelo fundamento legal que legitima o tratamento deve ser aferido de acordo com a finalidade que o tratamento de dados pretende cumprir. As empresas, no seu relacionamento com os clientes, devem fazer uma distinção entre o tratamento de dados efetuado no âmbito da contratação dos serviços solicitados pelo Cliente e, por exemplo, envio de conteúdos de caráter publicitário.

A Licitude de Tratamento pode ser dividida em:

2.3.1. Consentimento

O titular dos dados dá o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.
O responsável pelo tratamento deve obter do titular dos dados uma "declaração" de vontade livre, informada, explícita e inequívoca.
- Livre;
- Específico;
- Informado;
- Explícito.

O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, ação que deve ser tão fácil de retirar como foi de dar.

2.3.2. Relação contratual

O tratamento é necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados.

Exemplo:
- Para pagar o vencimento aos trabalhadores, os serviços têm de dispor de dados pessoais como o NIF e um número de conta bancária;
- Diligências pré-contratuais: pedido de simulação de prémio de seguro.

2.3.3. Cumprimento de obrigação legal

O tratamento é necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

Exemplo:
- Seguros obrigatórios;
- Emissão de fatura pela aquisição de bens e/ou prestação de serviços.

2.3.4. Interesse público e exercício de poderes públicos;

O tratamento é necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.

2.3.5. Interesses vitais

O tratamento é necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular.

2.3.6. Interesses legítimos do responsável

O tratamento é necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Só pode ser invocado depois de um teste de ponderação entre o interesse do responsável de tratamento de dados e os direitos do titular de dados. Caso seja esta a licitude de tratamento invocada, deverão ser descriminados os interesses com que o responsável de tratamento pretende justificar o tratamento.

2.4. Encarregado de proteção de dados

O *Data Protection Officer* (DPO) ou o Encarregado de Proteção de Dados (EPD) é um trabalhador ou consultor externo que tem como função principal:

- INFORMAR E ACONSELHAR o responsável pelo tratamento ou o subcontratante, bem como os seus trabalhadores, sobre as respetivas obrigações nos termos da lei da proteção de dados;

- CONTROLAR O CUMPRIMENTO, por parte da organização, de toda a legislação relacionada com a proteção de dados pessoais, nomeadamente em auditorias, atividades de sensibilização e formação do pessoal implicado nas operações de tratamento;

- PRESTAR ACONSELHAMENTO sempre que tenha sido realizada uma AIPD e controlar a sua realização;

- ATUAR COMO PONTO DE CONTACTO para pedidos de pessoas relativamente ao tratamento dos seus dados pessoais e ao exercício dos seus direitos;

- COOPERAR COM A AUTORIDADE DE CONTROLO e atuar como ponto de contacto das mesmas sobre questões relacionadas com o tratamento;

- ASSEGURAR A REALIZAÇÃO DE AUDITORIAS, quer periódicas, quer não programadas;

- SENSIBILIZAR OS UTILIZADORES para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança.

Para facilitar o exercício do direito de acesso, o responsável pelo tratamento deve disponibilizar publicamente os contactos do Encarregado de Proteção de Dados em todos os suportes de 1.º nível de recolha de informação.

2.4.1. Em que situações é que é obrigatório ter um Encarregado de proteção de dados?

A nomeação de um EPD torna-se obrigatória:

- Quando o tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

- Quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala;

- Quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º.

2.4.2. É preciso fazer algum registo do EPD?

Sim. Além da publicação dos contactos do encarregado de proteção de dados e dar conhecimento aos titulares dos dados desses contactos quando lhes presta as informações referidas nos artigos 13.º e 14.º do RGPD, também é necessário registar junto da CNPD essa informação. Para o efeito, a CNPD disponibiliza um formulário próprio. (Ir para o formulário).

2.5. Responsabilidades do responsável de tratamento

No âmbito do Regulamento, o responsável de tratamento deverá:

- Proceder ao registo das atividades de tratamento;
- Garantir a licitude do tratamento;
- Definir políticas, procedimentos, adequadas;
- Selecionar apenas fornecedores que ofereçam garantias de cumprimento do RGPD;
- Cooperar com as autoridades de controlo;
- Aplicar medidas técnicas e organizativas que garantam a segurança dos dados;
- Avaliar os riscos;
- Proceder à avaliação de impacto de proteção de dados;
- Em caso de violação, notificar a Autoridade de Controlo, em 72h.

2.6. Quem é a Autoridade de Controlo Portuguesa?

A Comissão Nacional de Proteção de Dados é a autoridade de controlo nacional que controla e fiscaliza o cumprimento do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, e da Lei n.º 58/2019 de 8 de agosto que assegura a execução na ordem jurídica nacional.

2.7. Montantes das Coimas

	Grandes Empresas	PMEs	Pessoas Singulares
Contraordenações Muito Graves	5000,00€ a 20.000.000,00€ ou 4% do volume de negócios anual, a nível mundial, conforme o que for mais elevado	€. 2000,00 a €. 2.000.000,00 ou 4% do volume de negócios anual, a nível mundial, conforme o que for mais elevado	1000,00€ a €. 500.000,00€
Contraordenações Graves	€. 2500,00 a €. 10.000.000,00 ou 2% do volume de negócios anual, a nível mundial	€. 1000,00 a €. 1.000.000,00 ou 2% do volume de negócios anual, a nível mundial	500,00€ a 250.000,00€

CAPÍTULO III

IMPLEMENTAÇÃO DA PROTEÇÃO DE DADOS

Para o processo de implementação deverão ser considerados os seguintes passos:

3.1. Inventariação dos dados

A implementação de um processo de proteção de dados seja eles pessoais ou não é inventaria-los. O mapeamento é essencial porque só conhecendo os dados que possuímos, os meios que dispomos, a medida técnica e organizativa de segurança dos dados é possível proteger os dados.

3.2. Verificação do cumprimento dos princípios

Para cada tratamento deve verificar-se se estão a ser cumpridos os princípios relativos ao tratamento de dados pessoais

3.3. Verificação da licitude do tratamento

Identificação do fundamento para o tratamento. Caso não exista deverão ser eliminados os dados pessoais e os tratamentos realizados ou iniciar de imediato os procedimentos para a sua legalização.

3.4. Revisão dos processos de recolha de dados

Consoante o fundamento jurídico para o tratamento de dados, seja o consentimento ou a execução de um contrato, devem ser revistos todos os formulários de consentimento e clausulados contratuais, por forma a ajustá-los às novas exigências do RGPD.

3.5. Atenção especial ao Consentimento

O consentimento deve ser dado de forma expressa, livre, informada e inequívoca de forma a demonstrar com clareza a intenção dos titulares dos dados. Sempre que possível deverão ser consideradas outras formas de licitude,
Deve existir sempre uma forma de ação afirmativa clara. O consentimento não pode ser deduzido através do silêncio, caixas com um "visto" prévio ou inatividade. O consentimento deve ainda estar separado de outros termos e condições e deverão também existir formas simples para as pessoas retirarem o consentimento.

No tratamento de dados que dependa de consentimento, verificar:

- Necessidade de o responsável de tratamento poder demonstrar que o titular consentiu;
- Quando dado no contexto de declaração escrita que inclua outros assuntos, analisar se o consentimento foi dado de forma distinta, de fácil acesso, em linguagem clara e simples;
- Possibilidade de retirar consentimento a qualquer momento e de forma tão fácil como foi dado;
- Dados de crianças até aos 13 anos apenas com o consentimento dos pais ou tutores legais no contexto de ofertas de serviços da sociedade de informação;
- Fornecimento de informação prévia ao tratamento, ou seja, no ato da recolha de dados pessoais, sobre:
  - Identidade do responsável pelo tratamento de dados;
  - Os fins a que o tratamento se destina;
  - Destinatários dos dados (quando são partilhados);
  - Intenção de fazer transferência para fora do Espaço Económico Europeu;
  - Salvaguarda dos direitos dos titulares sobre os dados pessoais que lhes dizem respeito que estão a ser tratados.

Nota: nos casos em que o tratamento sirva fins múltiplos, deverá ser dado consentimento para todos esses fins (um consentimento, separado, para cada uma das finalidades).

3.6. Revisão de subcontratos

Levantamento de todos os subcontratos (escritos ou não) em que há tratamento de dados pessoais. Todas as relações contratuais identificadas devem ser reduzidas a escrito, com o conteúdo mínimo exigido pelo RGPD. O recurso a subcontratantes só é possível se estes apresentarem garantias suficientes de execução de medidas técnicas e organizativas adequadas ao RGPD.

3.7. Definição da política de segurança

Criação e elaboração de uma política de segurança que seja do conhecimento de todos os colaboradores com medidas técnicas e organizativas físicas e digitais elencadas e definição de procedimentos internos que assegurem a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento de dados pessoais.

3.8. Criação de política e aviso de privacidade

As políticas e avisos de privacidade são documentos onde está descrita a forma como a organização recolhe, trata, armazena e protege os dados pessoais que recolhe de forma transparente diretamente junto dos titulares de dados ou através de organizações terceiras. As políticas de privacidade criadas deverão ter as seguintes informações.

3.8.1. Prestação de informação

Aquando da recolha de dados junto do titular dos dados, o responsável de tratamento deve prestar informação ao titular dos dados sobre:

- quem é a organização (os seus contactos e os do EPD, se existir);
- porque é que a sua organização irá utilizar os seus dados pessoais (finalidades);
- as categorias de dados pessoais em causa;
- a licitude para o tratamento dos seus dados;
- durante quanto tempo serão conservados os dados;
- quem mais poderá receber os dados;
- se os dados pessoais serão transferidos para um destinatário fora da UE;
- direito de acesso aos dados pessoais, bem como outros direitos básicos no domínio da proteção de dados;

- que a pessoa tem o direito de apresentar uma reclamação a uma autoridade de proteção de dados;
- que a pessoa tem o direito de retirar o seu consentimento em qualquer altura (se aplicável);
- se aplicável, a existência de decisões automatizadas e a lógica envolvida, incluindo as suas consequências.

Quando os dados pessoais não são recolhidos junto do titular, o responsável de tratamento deve:

- Comunicar as informações num «prazo razoável» após a obtenção dos dados pessoais e, o mais tardar, no prazo de um mês «tendo em conta as circunstâncias específicas em que estes forem tratados»;
- Na situação em que os dados se destinam a ser utilizados para fins de comunicação com o titular dos dados. As informações devem ser comunicadas o mais tardar no momento da primeira comunicação com o titular dos dados;
- A prestação de informação pelo responsável ao titular dos dados deve ser REGISTADA, de modo a garantir a prova dessa prestação por parte do responsável.

Não é exigível ao responsável pelo tratamento a prestação específica da informação ao titular dos dados quando:

- O titular dos dados já disponha dessa informação;
- O cumprimento dessa obrigação implique um esforço desproporcionado para o responsável pelo tratamento;
- A obtenção dos dados, bem como a sua transmissão, se encontre expressamente prevista no direito da união europeia ou em legislação nacional;
- Os dados se revistam natureza confidencial ou secreta, em decorrência do cumprimento de uma obrigação legal.

3.8.2. Como prestar esta informação ao titular de dados?

Existe no Regulamento uma tensão inerente entre, por um lado, os requisitos relativos ao fornecimento de informações exaustivas aos titulares dos dados e, por outro lado, os requisitos relativos à forma de o fazer, que deve ser concisa, transparente, inteligível e de fácil acesso.

No momento da recolha dos dados pessoais, devem ser prestadas informações sobre as finalidades do tratamento, a identidade do responsável pelo tratamento e uma listagem dos direitos dos titulares dos

dados ou outras informações com maior impacto que possam vir a surpreender o titular dos dados.

3.8.3. Métodos de recolha e prestação da informação

É fundamental que o(s) método(s) escolhido(s) para veicular as informações seja(m) adequado(s) às circunstâncias específicas, ou seja, a maneira como o responsável pelo tratamento e o titular dos dados interajam ou a maneira como as informações sobre o titular dos dados sejam recolhidas.

3.8.4. O caso de titulares vulneráveis

Se um responsável pelo tratamento está consciente de que os seus bens/serviços são utilizados por (ou se destinam a) outros membros vulneráveis da sociedade, incluindo pessoas com deficiência ou pessoas que possam ter dificuldade em aceder às informações, as vulnerabilidades desses titulares de dados devem ser tidas em consideração pelo responsável pelo tratamento na sua avaliação da forma como assegura o cumprimento das suas obrigações de transparência em relação a esses titulares de dados.

3.9. Criação do registo de atividades de tratamento

O registo das atividades de tratamento é uma obrigação imposta pelo artigo 30.º do RGPD para os responsáveis pelo tratamento e para os subcontratantes. O conteúdo dos registos é distinto consoante se trate de um responsável pelo tratamento ou de um subcontratante. Quando uma organização efetua tratamentos de dados enquanto responsável pelo tratamento e enquanto subcontratante, deve manter dois registos diferenciados.

Os registos são efetuados por escrito, incluindo em formato eletrónico, e são facultados à CNPD a seu pedido.

Estão dispensados do registo das atividades de tratamento empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados.

De modo a facilitar o cumprimento desta obrigação, em especial por parte das micro, pequenas e médias empresas, a CNPD disponibiliza um modelo de registo que pode ser utilizado para o efeito (Ver modelo de registo).

3.10. Criação de mecanismos de exercício dos direitos

As empresas devem criar e implementar mecanismos para dar resposta ao exercício dos direitos dos titulares:

3.10.1. Quais são os Direitos dos Titulares dos Dados?

Enunciam-se os direitos dos titulares de dados pessoais que devem ser garantidos pelo Responsável de Tratamento

- **Direito de informação**;

- **Direito a confirmação:** O titular dos dados tem direito de obter confirmação se os seus dados pessoais são ou não objeto de tratamento e, se for o caso, ter acesso:
  - Aos dados pessoais em causa;
  - Quais os fins do tratamento;
  - Quais os destinatários dos dados;
  - Qual o prazo de conservação dos dados;
  - Se os dados não tiverem sido recolhidos junto do titular, qual a origem desses dados;
  - Qual a forma de exigir a retificação ou apagamento dos dados.

- **Direito de retificação de dados inexatos:** O titular tem o direito de obter, sem demora injustificada a retificação ou atualização dos dados pessoais inexatos;

- **Direito ao apagamento ("direito a ser esquecido"):** O titular tem o direito de obter o apagamento dos seus dados pessoais, sem demora injustificada. O exercício do direito ao apagamento não pode afetar, designadamente:
  - O cumprimento de obrigações legais;
  - Razões de interesse público;
  - O tratamento para fins de arquivo público, investigação científica e histórica e fins estatísticos;
  - O exercício de direitos em processos judiciais;

- **Direito à limitação do tratamento:** O titular dos dados pode exigir junto do responsável pelo tratamento que o tratamento seja limitado;

- O titular de dados solicita a um banco que encerre todas as contas e que apague todos os seus dados pessoais. O banco está, contudo, sujeito a uma lei que obriga os bancos a conservarem todos os dados dos clientes durante dez anos. O banco é obrigado por lei a conservar os seus dados. Contudo, a pessoa pode solicitar a limitação do tratamento dos dados para garantir que estes não são utilizados acidentalmente para fins indesejados;

- **Direito de portabilidade:** O direito de portabilidade dos dados abrange apenas os dados fornecidos pelos respetivos titulares. A portabilidade dos dados deve, sempre que possível, ter lugar em formato aberto. (por exemplo, XML, JSON, CSV, etc.);

- **Direito de oposição:** O titular dos dados tem o direito de se opor, a qualquer momento, ao tratamento dos dados pessoais que lhe digam respeito, nomeadamente: tem o direito de se opor a qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar dados pessoais para avaliar e determinar características do titular dos dados;

- **Direito de queixa:** O titular dos dados tem o direito de apresentar queixa junto da Comissão Nacional de Proteção de Dados (CNPD), enquanto autoridade de controlo nacional;

- **Direito de indemnização:** Os titulares dos dados têm direito a ser indemnizados pelos danos que lhes sejam causados pela violação ou incumprimento do RGPD.

3.10.2. Como responder?

- A organização deve responder aos pedidos sem demora injustificada e, em princípio, no prazo de um mês a contar da receção do pedido;

- Confirmar se está ou não a efetuar o tratamento de dados pessoais que lhe digam respeito;

- Pode pedir informações suplementares para confirmar a identidade da pessoa que efetua o pedido;

- O tratamento dos pedidos das pessoas deve ser efetuado gratuitamente. Se os pedidos forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, é

possível cobrar uma taxa razoável ou recusar-se a dar seguimento ao pedido;

- Se a organização rejeitar o pedido, tem de informar a pessoa sobre os motivos para tal e sobre o direito de apresentar uma reclamação à autoridade de proteção de dados, bem como de intentar ação judicial;

- Manter um registo interno dos pedidos efetuados.

3.11. Realização de Avaliações de Impacto

Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve realizar uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

A realização de uma avaliação de impacto sobre a proteção de dados é obrigatória de acordo com o RGPD no caso:

- Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

- Operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações;

- Controlo sistemático de zonas acessíveis ao público em grande escala.

A CNPD publicou igualmente uma lista em que é obrigatória a realização da avaliação de impacto e que resumidamente aqui se apresenta:

- Tratamento de informação decorrente da utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde;

- Interconexão de dados pessoais ou tratamento que relacione dados pessoais de categorias especiais ou dados de natureza altamente pessoal;

- Tratamento de dados pessoais de categorias especiais ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível assegurar o direito de informação;

- Tratamento de dados pessoais que implique ou consista na criação de perfis em grande escala;

- Tratamento de dados pessoais que permita rastrear a localização ou os comportamentos dos respetivos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação destes, exceto quando o tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos;

- Tratamento dos dados de categorias especiais ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público, investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que apresente garantias adequadas dos direitos dos titulares;

- Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;

- Tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados. Tratamento de dados pessoais de categorias especiais ou dados de natureza altamente pessoal com utilização de novas tecnologias ou nova utilização de tecnologias já existentes.

3.12. Criação de procedimentos para notificação de violações de dados pessoais

Quando uma organização sofre uma violação de dados pessoais que resulta na quebra de confidencialidade, disponibilidade ou integridade dos mesmos e se a violação for suscetível de representar um risco para os direitos e as liberdades pessoais, a organização tem de notificar a autoridade de controlo sem demora injustificada e, o mais tardar, no prazo de 72 horas após tomar conhecimento da violação. Assim, é necessário que a organização disponha de procedimentos definidos com atribuição de papeis e responsabilidades que perante uma situação de emergência possa responder sem demoras em tempo útil e de forma eficaz que para tomar medidas de segurança quer para efetuar a comunicação à CNPD.

A CNPD tem disponível um formulário na página para comunicação de violação de dados.

DOCUMENTAÇÃO DE REFERÊNCIA

- Comissão Nacional de Proteção de dados - https://www.cnpd.pt/
- REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016
- Lei n.º 58/2019 de 8 de agosto
- Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados
- Gabinete Nacional de Segurança
- Cartilha de Segurança para a Internet - https://cartilha.cert.br/privacidade/

ANEXOS

Política de Privacidade

QUEM SOMOS?

A Organização XPTO, compra e venda de imóveis, LDA é uma sociedade comercial por quotas, pessoa coletiva nº 5..... com sede na Rua António ....., nº300, Lisboa.
Esta sociedade dedica-se a, segundo os códigos de atividade económica x e x.

O NOSSO COMPROMISSO PARA COM OS SEUS DADOS

A Organização XPTO, dedicada a…, assumiu o compromisso de proteger a privacidade da informação pessoal por si recolhida e tratada.
Na nossa empresa o tratamento dos dados pessoais é realizado no estrito cumprimento do Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção de pessoas físicas no que diz respeito ao processamento de dados pessoais e sobre a livre circulação de tais dados, e/ou qualquer legislação que regule, adite ou substitua a referida legislação, no conjunto designado por Regulação sobre Proteção de Dados Pessoais (doravante referido como RGPD).

QUEM É O RESPONSÁVEL PELA RECOLHA E TRATAMENTOS DOS SEUS DADOS PESSOAIS?

A nossa empresa é a entidade responsável pela recolha e tratamento dos dados pessoais, que no âmbito da relação contratual ou pré-contratual, e de acordo com o serviço solicitado, irá recolher e tratar os dados pessoais imprescindíveis para a realização desse fim.

QUE DADOS SEUS GUARDAMOS?

A nossa empresa recolhe dados pessoais dos clientes no âmbito de uma relação contratual ou pré-contratual; e apenas são recolhidos os dados pessoais estritamente necessários ao cumprimento dessa finalidade; nomeadamente: nome, género, nacionalidade, data de nascimento, contribuinte fiscal, estado civil e regime de bens no caso de casado, número de cartão de cidadão e respetiva validade, número de passaporte e respetiva validade, cartão de autorização de residência, morada, contacto telefónico e endereço eletrónico, declarações de IRS, nota de liquidação de IRS, recibos de vencimento, contratos de trabalho, apólices de seguro, Número de Identificação Bancário, Número de Conta Bancário, Senha Eletrónica das Finanças, Contratos de arrendamento, escrituras públicas, procurações, certificados energéticos, fichas técnicas, licenças de habitabilidade e todos os documentos inerentes aos prédios administrados.
Em nenhuma situação será solicitada informação sobre convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica bem como os dados relativos à saúde e à vida sexual, incluindo os dados genéticos.

QUAIS SÃO AS FORMAS DE RECOLHA DE DADOS PESSOAIS QUE UTILIZAMOS?

Os dados pessoais podem ser recolhidos através de e-mail, contacto telefónico ou presencialmente no nosso escritório, mediante o prévio consentimento do cliente. Por regra, os dados pessoais são recolhidos no âmbito de uma relação contratual ou pré-contratual com o cliente; ou seja, mediante a sua solicitação de um serviço.
Alguns dados pessoais são de fornecimento obrigatório e, em caso de falta ou insuficiência desses dados, a nossa empresa não poderá prestar o serviço em causa, pelo que informará os clientes da natureza obrigatória do fornecimento dos dados.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Os dados pessoais recolhidos são tratados informaticamente e no estrito cumprimento da legislação de proteção de dados, sendo armazenados em base de dados específicas, criadas para o efeito e, em situação alguma, os dados recolhidos serão utilizados para outra finalidade que não seja aquela para a qual foi dado o consentimento por parte do titular dos dados.
Os dados recolhidos poderão ser transmitidos aos proprietários dos prédios administrados pela nossa empresa, durante ou após a vigência do contrato de administração dos referidos imóveis.

QUAIS AS FINALIDADES DO TRATAMENTO DOS DADOS PESSOAIS?
Os Dados Pessoais são obtidos com as seguintes finalidades:

Execução do contrato:
A solicitação dos clientes, e com os dados pessoais fornecidos para esse efeito, a nossa empresa procede à prestação de serviços contratados; nomeadamente, arrendamento e compra e venda de imóveis e/ou administração de condomínios.

Informações:
Recrutamento: Os dados pessoais constantes em currículos e cartas de apresentação enviadas por email ou entregues no nosso escritório, serão tratados por nós. Os currículos de candidatos que não apresentem as aptidões ou habilitações necessárias para o exercício das funções a que se candidatam serão destruídos no prazo máximo de 1 (uma) semana. Os restantes serão guardados pelo período máximo de 2 (dois) anos, findo o qual serão destruídos.
Se o responsável pelo tratamento de dados celebrar um contrato de trabalho com um dos candidatos, os dados recolhidos no processo de recrutamento/candidatura serão armazenados com a finalidade de elaborar o contrato de trabalho e para todas as finalidades legais de carater obrigatório.

Videovigilância:
O nosso escritório possui instalado um sistema de videovigilância para proteção de pessoas e bens, procedendo à gravação de imagens as quais são conservadas por um período de 30 (trinta) dias, findo o qual, serão as mesmas destruídas, sem prejuízo da conservação por período superior, por ordem judicial ou solicitação de órgão de polícia criminal no âmbito de processo crime.

QUAIS OS FUNDAMENTOS JURÍDICOS PARA O TRATAMENTO DOS DADOS PESSOAIS?
Nos termos da legislação de proteção de dados vigente na União Europeia (o Regulamento Geral sobre a Proteção de Dados) a utilização de dados pessoais tem de justificar-se ao abrigo de, pelo menos, um destes fundamentos jurídicos para o tratamento de dados pessoais:

a) Quando foi dado o consentimento claro, expresso e inequívoco por parte do cliente, o qual poderá ser retirado em qualquer altura.

b) Quando o tratamento dos dados pessoais é imprescindível à execução de um contrato;

c) Quando o tratamento seja necessário para cumprimento das obrigações legais;

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

d) Quando o tratamento seja necessário para alcançar um interesse legítimo;

e) Quando o tratamento for necessário para que possamos declarar, exercer ou defender um direito num processo judicial contra si, nós ou um terceiro.

EM QUE CIRCUNSTÂNCIAS EXISTE COMUNICAÇÃO DE DADOS A OUTRAS ENTIDADES (TERCEIROS E SUBCONTRATADOS)?

a) Ao fornecerem os seus dados pessoais, os clientes declaram que autorizam e consentem que os mesmos sejam tratados pela nossa empresa. Bem como, consente o cliente, que os seus dados pessoais sejam transmitidos /comunicados pela nossa empresa aos proprietários dos bens imóveis por nós administrados, em conformidade com o RGPD, bem como a Companhias de Seguros para celebração de contratos de seguro multirriscos das frações cujo condomínio seja por nós administrado e na medida do estritamente necessário para a concretização do serviço prestado.

b) Na eventualidade de não concordar com a consulta e tratamentos dos seus dados pessoais nas condições supra descritas no âmbito da relação contratual, a nossa empresa não poderá contratar consigo, na medida em que os dados solicitados são absolutamente indispensáveis para a prestação do serviço que pretende contratar connosco.
c) A nossa empresa procede ao tratamento e conservação de dados pessoais dos seus clientes através de sistemas de faturação denominados em cloud. As empresas detentoras destes programas, e outros softwares na qualidade de subcontratantes comprometeram-se com a nossa empresa ao rigoroso cumprimento do RGPD.

QUANDO É QUE PODERÁ OCORRER FORNECIMENTO DE DADOS A TERCEIROS?

No decurso de uma investigação, denúncia ou procedimento, às Autoridades fiscais, de auditoria, aos Organismos Públicos, ao Tribunal e às Forças de Segurança responsáveis. No âmbito da atividade de administração de condomínio poderão ser transmitidos os dados pessoais dos clientes a companhias de seguro para efeitos de contrato de seguro multirriscos das frações dos quais são proprietários.

WEBSITE

A visualização e utilização das páginas do nosso website é permitida sem que para isso tenha que indicar algum tipo de dados pessoais, contudo, se um titular de dados quiser usar os serviços disponibilizados através do nosso website, poderão ser requisitados e tratados dados pessoais deste utilizador.
Como responsável pelo tratamento de dados, a nossa empresa implementou inúmeras medidas técnicas e organizacionais para garantir a proteção dos dados pessoais tratados através deste website.
O nosso site recolhe uma série de dados e informações gerais quando um titular de dados acede ao site.
Esses dados e informações gerais são armazenados nos arquivos de log do servidor.

INSCRIÇÃO NO WEBSITE

O titular dos dados tem a possibilidade de se registar no site da empresa com a indicação dos dados pessoais que são solicitados no preenchimento do formulário usado para registo.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Os dados pessoais fornecidos são para efeito de consulta e obtenção de informações disponibilizadas no nosso site sobre a administração do condomínio do prédio onde o detentor dos dados pessoais habita e no âmbito do contrato de prestação de serviços celebrado com a nossa empresa ou ainda para obter informações sobre algum imóvel cuja venda ou arrendamento esteja a ser publicitada no nosso website.
Pelo que, os dados pessoais recolhidos são tratados apenas internamente não sendo transmitidos a terceiros.
As pessoas registadas têm liberdade para alterar os dados pessoais especificados durante o registo a qualquer momento, ou para que sejam completamente excluídos da base de dados do responsável pelo tratamento de dados.

PEDIDOS DE CONTACTO PELO WEBSITE

O nosso website contém informações que permitem um rápido contato eletrónico com a nossa empresa, bem como a comunicação direta connosco, que também inclui um endereço de e-mail. Se um titular dos dados entrar em contacto com o responsável pelos dados por e-mail ou por meio de um formulário de contato, os dados pessoais transmitidos pela pessoa em questão serão armazenados automaticamente. Esses dados pessoais transmitidos voluntariamente por um titular de dados ao responsável pelos dados são armazenados com o objetivo de tratar ou contactar o titular dos dados. Não há transferência desses dados pessoais para terceiros.

REDE SOCIAL "FACEBOOK"

O Facebook recolhe informação de que página especifica do nosso site foi visitado pelo utilizador.
Se o titular dos dados estiver ligado ao mesmo tempo no Facebook, o Facebook detetará todas as ligações para o nosso site pelo detentor de dados – e por todo o tempo da visita do utilizador no nosso website – assim como que páginas especificas foram visitadas pela pessoa em causa.
Essas informações são recolhidas através das ferramentas do Facebook e associadas à respetiva conta do Facebook do titular dos dados.
Se a pessoa em causa clicar num dos botões do Facebook integrados no nosso website, por exemplo o botão "Gostar", ou se o titular dos dados enviar um comentário, o Facebook corresponderá essa informação à conta de usuário pessoal do Facebook do titular dos dados e armazenará os dados pessoais.
O Facebook irá receber continuamente, através das ferramentas do Facebook, informações sobre as visitas ao site, feitas pelo titular dos dados, desde que o titular de dos esteja ligado no Facebook durante o período de visita ao site.
Este processo irá ocorrer independentemente do sujeito clicar no ícone do Facebook ou não.
A diretriz de proteção de dados publicada pelo Facebook, disponível em facebook.com/about/privacy/, fornece informações sobre a recolha, tratamento e uso de dados pessoais pelo Facebook. Além disso, são explicadas as opções de configuração oferecidas pelo Facebook para proteger a privacidade dos dados.

GOOGLE ANALYTICS

No nosso site, o responsável pelo tratamento de dados integrou o componente do Google Analytics com a função de anonimização.
Web analytics é o processo de recolha e análise de dados sobre o comportamento dos visitantes dos sites.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Para a análise da web por meio do Google Analytics, o responsável de dados usa o aplicativo "_gat._anonymizelp". Por meio deste aplicativo, o endereço IP da conexão de Internet do titular dos dados e informações recolhidas, entre outros, para avaliar o uso do site da Improxy e para fornecer relatórios on-line, que mostram as atividades no site e para fornecer outros serviços relacionados ao uso do site na Internet.

O titular dos dados pode, como dito acima, impedir a configuração de cookies no site, a qualquer momento, por meio de ajuste correspondente no navegador da web que utilizar e, assim, negar permanentemente a configuração de cookies.
Tal ajuste no navegador da Internet usado também impedirá que o Google Analytics instale um cookie no sistema de tecnologia de informação do utilizador.
Além disso, o titular dos dados tem a possibilidade de se opor a uma recolha de dados que são gerados pelo Google Analytics, relacionado ao usso deste site, bem como o tratamento desses dados pelo Google. Para tal, o titular dos dados deve descarregar um complemento ao navegador no link https://tools.google.com/dlpage/gaoptout e instalá-lo.

COMO É QUE SE PROCEDE AO TRATAMENTO DOS SEUS DADOS PESSOAIS?

1- A nossa empresa, acedendo a qualquer dado pessoal, compromete-se a:
a) Proteger, por intermédio de medidas de segurança, legalmente exigíveis, de natureza técnica e organizacional, que garanta a sua segurança, evitando assim a sua alteração, perda, tratamento ou acesso não autorizado, em conformidade com o estado da tecnologia em cada momento, a natureza dos dados e os possíveis riscos a que estejam expostos;
b) Utilizar ou aplicar os dados exclusivamente com as finalidades devidamente previstas;
c) Certificar-se de que os dados são acedidos e tratados unicamente pelos trabalhadores cuja intervenção seja necessária para a prestação do serviço, estando os mesmos obrigados ao dever de sigilo e confidencialidade.

2- Ao fornecer os seus dados pessoais, os titulares dos mesmos, ou terceiros devidamente autorizados para o efeito, declaram que autorizam e consentem no tratamento desses dados pela nossa empresa para as finalidades de facilitar e permitir a prestação de serviços contratados.

3- A nossa empresa declara e garante que implementou, está dotada e continuará a implementar as medidas de segurança de natureza técnica e organizacional necessárias para garantir a segurança dos dados de carater pessoal que lhe sejam fornecidos, visando evitar a sua alteração, perda, tratamento e/ou acesso não autorizado, tendo em conta o estado atual da tecnologia, a natureza dos dados armazenados e os riscos a que estão expostos.

4- A nossa empresa é responsável pelo tratamento dos dados por si recolhidos.

5- O acesso à informação em arquivo por parte dos colaboradores da nossa empresa só é possível com a inserção de senhas de acesso.

6- Os dados pessoais são tratados com o grau de proteção legalmente exigível para garantir a segurança dos mesmos e evitar a sua alteração, perda, tratamento ou acesso não autorizado, estando o titular dos mesmos consciente e aceitando que as medidas de segurança em Internet não são inexpugnáveis, tendo em conta o estado da tecnologia.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

8- Documentação cedida em suporte físico é cuidadosamente guardada com acesso condicionado e controlado pelo responsável da mesma. Sempre que não se torne necessário o seu arquivo os documentos são destruídos de forma irreversível.

DE QUE MODO SALVAGUARDAMOS OS SEUS DADOS PESSOAIS?

Estamos empenhados em adotar todas as medidas razoáveis e apropriadas para proteger as informações pessoais que possuímos de utilização indevida, alterações acidentais, ou ilícitas, perda e divulgação ou acessos não autorizados. Para o efeito, a nossa empresa utiliza sistemas de segurança, regras e outros procedimentos de modo a garantir a proteção dos seus dados pessoais, bem como para prevenir o acesso não autorizado aos dados, o uso impróprio, a sua divulgação, perda ou destruição.

POR QUANTO TEMPO CONSERVAMOS OS SEUS DADOS PESSOAIS?

Só guardamos os seus dados pessoais pelo tempo necessário para atingir a finalidade para a qual os recolhemos, para responder às suas necessidades, às solicitações que nos dirigir, ou para cumprir com as nossas obrigações contratuais e legais.
Para determinar o período pelo qual guardamos os seus dados, usamos os critérios referidos infra. Caso se apliquem vários critérios simultaneamente, conservaremos os seus dados pessoais nos termos do critério que implicar a conservação dos seus dados pessoais pelo maior período de tempo.

1. Quando contratar os serviços da nossa empresa, os seus dados serão conservados durante a vigência da nossa relação comercial, incluindo eventuais reclamações que possam surgir, bem como e pelo período de 5 anos após a cessação de tal relação, sem prejuízo do cumprimento de obrigações legais do responsável do tratamento;

2. Quando nos fornecer os seus dados pessoais no âmbito de um contrato celebrado com os nossos clientes (por nosso intermédio) conservaremos os seus dados pessoais durante a vigência do aludido contrato e durante 5 anos após a sua cessação.

3. Quando nos fornecer os seus dados no âmbito de uma relação pré-contratual e não se celebrar qualquer contrato, conservaremos os seus dados pelo período de 30 (trinta) dias, findo o qual serão os mesmos destruídos.

4. Se nos contactar para colocar questões, solicitar informações e esclarecimentos, conservaremos os seus dados pessoais pelo período de tempo necessário para resolver a sua questão/prestar-lhe informações e/ou esclarecimentos solicitados;

5. Relativamente às imagens captadas pelo sistema de videovigilância instalado no nosso escritório, serão conservadas durante o prazo máximo de 30 (trinta) dias;

6. Relativamente aos dados recolhidos no processo de recrutamento, durante o prazo máximo 2 anos após o encerramento do processo de recrutamento;

DE QUE FORMA PODE ACEDER, ALTERAR OU REMOVER OS DADOS PESSOAIS QUE NOS FORNECEU?

Procuraremos tratar o seu pedido sem atrasos indevidos e, em qualquer caso, no prazo de um mês (sujeito a quaisquer prorrogações permitidas por lei).

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Tenha em atenção que poderemos manter um registo das suas comunicações (e-mail) para nos ajudar a resolver quaisquer questões suscitadas por si.

a) **Direito de se opor:** este direito permite-lhe opor-se ao tratamento dos seus dados pessoais por motivos relacionados com a sua situação particular, quando os seus dados sejam tratados por uma das seguintes razões: para prossecução dos nossos interesses legítimos, no exercício de funções de interesse público, para fins científicos, históricos, de investigação ou estatísticos. Neste caso, iremos pôr termo ao tratamento dos dados a cujo tratamento se opôs, salvo se pudermos demonstrar que temos motivos legítimos obrigatórios para o tratamento que se sobrepõem aos seus interesses ou estarmos a proceder ao tratamento dos seus dados no exercício ou defesa de um direito.

b) **Direito de retirar o consentimento**: caso tenhamos obtido o seu consentimento para proceder ao tratamento dos seus dados pessoais para determinadas atividades (por exemplo, para fins de marketing) poderá retirar esse consentimento em qualquer altura e deixaremos de realizar a atividade específica que anteriormente consentiu.

c) **Pedido de acesso aos dados**: poderá pedir-nos, em qualquer altura, que confirmemos as informações que dispomos sobre si, bem como solicitar informação adicional sobre as finalidades de tratamento, o prazo de conservação dos seus dados, entre outra informação prevista no artº 15º do RGPD.

d) **Direito ao esquecimento/apagamento**: em determinadas circunstâncias, tem o direito que apaguemos os seus dados pessoais. Normalmente, o exercício deste direito deve observar um dos seguintes critérios:
- Os dados já não são necessários para a finalidade para a qual os recolhemos/ tratamos.
- Quando tenha retirado o seu consentimento para procedermos ao tratamento dos seus dados e não exista outra razão válida para que os continuemos a tratar.
- Caso se oponha ao tratamento e não existam interesses legítimos prevalecentes que o justifiquem.

e) **Direito à limitação do tratamento**: em determinadas circunstâncias tem o direito de restringir o tratamento que damos ao aos seus dados pessoais. Caso tenhamos partilhado os seus dados pessoais com terceiros, estes serão notificados sobre o tratamento restringido, salvo se tal for impossível ou implicar um esforço desproporcionado. Iremos, naturalmente, notificá-lo antes de levantar qualquer restrição ao tratamento dos seus dados pessoais.

f) **Direito de retificação**: tem o direito de pedir que retifiquemos quaisquer dados pessoais inexatos ou incompletos que possuímos sobre si. Caso tenhamos partilhado esses dados pessoais com terceiros, estes serão notificados sobre a retificação. Quando apropriado, também lhe revelaremos a que terceiros divulgamos os dados pessoais inexatos ou incompletos. Nos casos em que consideremos que é razoável não satisfazermos o seu pedido, explicaremos os motivos da decisão. É importante que a informação pessoal que possuímos sobre si seja precisa e atual. Informe-nos caso haja alterações às suas informações pessoais durante o período em que conservamos os seus dados.
g) **Direito à portabilidade dos dados**: se assim o pretender, tem o direito de transferir os seus dados pessoais entre responsáveis pelo tratamento.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

2- Se desejar exercer os seus direitos de acesso, retificação, apagamento, portabilidade ou limitação do tratamento que o RGPD lhe concede, poderá remeter uma mensagem de correio eletrónico para rgpd@organização.com ou contactar o nosso escritório onde forneceu os seus dados.

3- Caso retire o seu consentimento, tal não compromete a licitude do tratamento efetuado até essa data.

DIREITO DE APRESENTAR RECLAMAÇÃO JUNTO DA AUTORIDADE DE CONTROLO

Caso esteja insatisfeito com a nossa utilização dos seus dados pessoais ou com a nossa resposta após o exercício de algum destes direitos, tem o direito de apresentar reclamação junto da sua autoridade de controlo (Comissão Nacional de Proteção de Dados – CNPD | Rua de São Bento, n.º 148, 3º, 1200-821 Lisboa | Tel: 351 213928400 | Fax: +351 213976832 | e-mail: geral@cnpd.pt).

DIREITO DE APRESENTAR RECLAMAÇÃO JUNTO DA AUTORIDADE DE CONTROLO

A nossa empresa reserva o direito de, a qualquer momento, proceder a reajustamentos ou alterações à sua Política de Privacidade, sempre no estrito cumprimento da Lei, sendo essas alterações devidamente divulgadas, de fora a mantê-lo sempre informado sobre a forma como tratamos os seus dados pessoais.

GARANTIAS E ADVERTÊNCIAS:

O titular dos dados garante que os dados pessoais comunicados à nossa empresa são certos e exatos e compromete-se a notificar qualquer alteração ou modificação aos mesmos e assume responsabilidade exclusiva pelas perdas e danos causados pela comunicação errónea, inexata ou incompleta dos dados.

COMO USAMOS OS "COOKIES"?

"Cookies" são pequenos ficheiros de texto que são armazenados no seu computador ou no seu dispositivo móvel através do navegador de internet (browser), retendo apenas informação relacionada com as suas preferências, não incluindo, como tal, os seus dados pessoais.

A colocação de cookies ajudará o website a reconhecer o seu dispositivo na próxima vez que o visitar. O nosso site utiliza cookies para melhorar a sua experiência de navegação e para fins de marketing.

Os cookies utilizados não recolhem informação que o poderá identificar.

Os cookies recolhem informações genéricas, como por exemplo, a forma como chega e utiliza o website ou a zona do país através do qual acede ao website.

Os cookies retêm apenas informação relacionada com as suas preferências, a qualquer momento pode, através do seu navegador de internet (browser), decidir ser notificado sobre a receção de cookies, bem como bloquear a respetiva entrada no seu sistema.

Porém, a recusa de uso de cookies no website resulta na impossibilidade de ter acesso ao mesmo.

Os cookies servem para ajudar a determinar a utilidade, interesse e o número de utilizações do website, permitindo uma navegação mais rápida e eficiente, bem como, analisar tráfego com o objetivo de melhorar o nosso serviço.

As definições de cookies podem ser alteradas nas preferências do seu navegador.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Para outros navegadores de internet (browsers), por favor, procure no menu "ajuda" do navegador (browser) ou contacte o fornecedor do navegador.
A nossa empresa agradece os seus comentários/sugestões em relação a esta Política de Privacidade. Contacte-nos: rgpd@organização.com

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Formulário de Consentimento

Nome: _____

E-mail: _____

Contacto Telefónico: _____

Mediante o meu consentimento, os meus dados pessoais poderão ainda ser tratados para (assinalar as opções pretendidas):

□ Envio de promoções através de e-mail.

□ Realização de inquéritos de avaliação de satisfação de clientes.

□ …

O Organização XPTO informa que poderá exercer o direito ao esquecimento e retirar o consentimento a qualquer momento, dispondo de formulário para o efeito no site www----------/, onde poderá consultar a nossa Política de Privacidade.

Data: ___/___/_____

Ass: _____ (Assinatura conforme Documento de Identificação)

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Formulário para exercício dos direitos dos titulares dos dados

REQUERENTE

Nome:_____

Doc. Identificação _____ Núm do docum._____

Telefone_____ E-mail _____

Autorizo a ser notificado(a) para o e-mail indicado.
Venho requerer o exercício do direito, abaixo indicado, ao abrigo do Regulamento Geral de Proteção de Dados RGPD:

- ☐ *Direito de acesso*
- ☐ *Direito de retificação*
- ☐ *Direito de apagamento*
- ☐ *Direito de limitação de tratamento*
- ☐ *Direito de portabilidade*
- ☐ *Oposição à tomada de decisão e criação de perfil automatizados*
- ☐ *Retirada de consentimento*

Pretendo que o direito seja exercido da seguinte forma:

Informa que a finalidade do tratamento dos dados pessoais aqui recolhidos, são única e exclusivamente, para o exercício dos direitos previstos no art. 13.º do RGPD.

Data _____ Assinatura _____

[Como parte de sua atividade, a organização pode exigir confidencialidade que seus funcionários acedam e tratem informações confidenciais, tanto internamente como em nome dos seus clientes, para os quais prestam serviços de tratamento de dados.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Este é um modelo acordo de confidencialidade, que pode ser usado como ponto de partida para a criação de um contrato personalizado adequado às circunstâncias específicas envolvidas. Note que deve procurar aconselhamento jurídico para a celebração do acordo, a fim de garantir que a redação usada seja adequada e o contrato válido].

Modelo de Acordo de Confidencialidade

……., nascido em ../../…., residente……, portador do Cartão de Cidadão nº……., válido até …/…/….., beneficiário da Segurança Social nº……, NIF: ……; por ter tido acesso a dados pessoais recolhidos pela empresa …….. (sua entidade empregadora), no âmbito do contrato de trabalho com aquela celebrado,

1º

Na vigência da sua relação laboral com o Responsável pelo Tratamento de dados e até dois anos após a cessação do contrato de trabalho, deverá guardar sigilo absoluto sobre quaisquer informações ou conhecimentos de natureza técnica, empresarial ou outra, adquiridos, necessária ou involuntariamente, durante a relação laboral ou por causa desta, respeitantes à Empregadora ou a quaisquer outras pessoas, singulares ou coletivas, que com estas se relacionem, nomeadamente administradores, diretores,
outros trabalhadores, clientes, parceiros e fornecedores.

2º

Reconhece e aceita a proibição de efetuar quaisquer reproduções, cópias, modificações, comunicações públicas, distribuição, ou qualquer outro tipo de cedência, gratuita ou onerosa de quaisquer documentos, incluindo programas informáticos, base de dados de clientes, publicações, informações contidas em bases de dados, na "intranet", em qualquer tipo de comunicação interna ou nas redes informáticas, ou qualquer outro material intelectual pertencente ou relativo à empregadora ou a qualquer terceiro que com esta se relacione, nomeadamente clientes e parceiros.

3º

Compromete-se a abster-se de exercer qualquer outra atividade, remunerada ou não, por conta própria ou alheia, ao abrigo de contrato de trabalho, contrato de prestação de serviços, nos quais pode utilizar ou recorrer aos dados pessoais a que tenha acesso por esta via.

4º

Compromete-se a não aceitar quaisquer comissões, prémios ou gratificações de quaisquer terceiros com os quais o Responsável pelo Tratamento mantenha relações comerciais, profissionais ou de parceria.

5º

Aceita cumprir e respeitar os procedimentos de segurança da informação, política de privacidade, código de conduta, regulamento interno em vigor em cada momento na sua entidade empregadora / responsável pelo tratamento de dados.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

6º

O incumprimento das obrigações suprarreferidas implicará o pagamento de uma indemnização no âmbito da responsabilidade civil, pelos prejuízos patrimoniais e/ou não patrimoniais sofridos pelo responsável pelo tratamento de dados ou terceiros.

7º

Reconhece que o endereço de correio eletrónico que utiliza ----------@----------.pt é para fins estritamente profissionais, reconhecendo ser de extrema importância que o seu nome figure no mesmo, assim como, em cartões de visita por considerar ser necessário para prossecução dos interesses legítimos da entidade empregadora /responsável pelo tratamento (alínea f) do nº1 do Artº6º do RGPD)

8º

Declara e reconhece que todos os equipamentos e serviços eletrónicos, informáticos e de comunicação, nomeadamente computadores, impressoras, telefones, telemóveis, endereços de correio eletrónico e acessos à internet têm como finalidade a sua utilização para fins profissionais.

9º

Quando terminar o contrato de trabalho obriga-se a entregar todos os objetos e equipamentos que tenha em seu poder, sob pena de incorrer em responsabilidade civil.

10º

Reconhece expressamente que a entidade empregadora /o Responsável pelo tratamento recolhe e detém os seus dados pessoais nos termos das alíneas b), c) e f) do nº1 do Artº6º do RGPD, nomeadamente, para efeitos da execução do contrato de trabalho, para cumprimento de obrigações legais e para prosseguimentos dos interesses legítimos do responsável pelo tratamento.

11º

Declara que tem conhecimento do direito a aceder aos seus dados pessoais junto do Responsável pelo tratamento dos mesmos, bem como, que os seus dados são transmitidos a subcontratantes, nomeadamente para efeitos de medicina no trabalho, seguro de acidentes de trabalho, processamento de salários, finanças e segurança social.

Data
O Declarante,

_____

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Acordo de proteção de dados entre responsável de tratamento e subcontratante

ENTRE:
PRIMEIRO OUTORGANTE: _____, **LDA**, NIPC: 513……., com sede na Rua……, Lisboa, aqui representada pelos seus sócios gerentes, _____ e _____, sócios gerentes, na qualidade de Responsável pelo tratamento de dados, e ----------

SEGUNDO OUTORGANTE: **……., LDA**, NIPC: ---------, com sede na ----------, Lisboa, aqui representada pelo seu sócio gerente, na qualidade de Subcontratante. ----------

Entre as partes outorgantes é estabelecida a seguinte política de proteção de dados, sujeita no seu cumprimento aos seguintes termos:

1º

A Segunda Outorgante presta serviços de contabilidade à Primeira Outorgante, tendo no âmbito dessa atividade acesso aos seguintes dados dos trabalhadores: nome, morada, número de telefone, número de identificação bancária, nome do cônjuge, nome de dependentes, números de identificação fiscal, NISS, vencimentos, abonos, subsídios e outras prestações recebidas, certificados de incapacidade de trabalho, baixas médicas, justificações de falta, registos de faltas, períodos de férias, filiação sindical, com a finalidade de proceder ao processamento de salários.

2º

Os referidos dados dizem respeito aos colaboradores, trabalhadores e prestadores de serviços à Primeira Outorgante, bem como aos membros dos órgãos sociais.

3º

O tratamento dos referidos dados é de natureza obrigatória para efeitos de cumprimento da Lei, nomeadamente envio de declarações de remunerações à segurança social e entrega de recibo de retribuição ao trabalhador, nos termos do disposto no artº13º do Decreto Regulamentar nº1-A/2011 de 3 de janeiro e Artº 276º do Código de Trabalho.

4º

O Primeiro Outorgante transmitirá ainda ao Segundo Outorgante dados pessoais dos seus clientes; nomeadamente, nome, morada e contribuinte fiscal que constam nas faturas emitidas pelo Responsável pelo tratamento com a única finalidade de apresentação de declarações fiscais junto da Autoridade Tributária Aduaneira para cumprimento da lei.

5º

O Segundo Outorgante, na qualidade de subcontratante, garante que os seus colaboradores/funcionários autorizados a tratar dos dados pessoais transmitidos pelo Primeiro Outorgante, assumiram um compromisso de confidencialidade ou estão sujeitas e adequadas obrigações legais de confidencialidade.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

6º

O Segundo Outorgante declara que aplicará as medidas técnicas e organizativas adequadas a assegurar um nível de segurança adequado ao risco, nomeadamente:

a) A pseudonomização e a cifragem de dados pessoais

b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

c) Capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico.

d) Tem um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

7º

O Segundo Outorgante compromete-se a não contratar outro subcontratante sem autorização expressa do responsável pelo tratamento, obrigando-se ainda a cumprir com o Regulamento de Proteção de Dados Pessoais e a Lei em matéria de proteção e dados pessoais.

8º

O Segundo Outorgante compromete-se ainda junto do Primeiro Outorgante a:

a) Prestar assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos;

b) Prestar assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações de segurança no tratamento, notificação à autoridade de controlo e aos titulares em caso de violação de dados pessoais, avaliação de impacto sobre a proteção de dados e consulta prévia, tal como previstas nos artigos 32.º a 36.º, tendo em conta a natureza de tratamento e a informação ao dispor do subcontratante;

c) Dependendo da opção do responsável pelo tratamento, apagará ou devolverá todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros; e

d) Disponibilizará ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações que impendem sobre o subcontratante e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor para este mandatado; e
e) Compromete-se a informar imediatamente o responsável pelo tratamento se considerar que alguma instrução viola o RGPD ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

9º

O tratamento dos dados pessoais, objeto do presente acordo terá a duração do contrato de prestação de serviços celebrado entre Primeiro e Segundo Outorgantes, findo o qual, os dados serão devolvidos ao Primeiro Outorgante, apagando-se as cópias existentes, a menos que a conservação dos dados seja exigida por força da Lei.

10º

É acordado ainda que o Segundo Outorgante responderá a todos os pedidos de informação e consulta do Primeiro Outorgante e não impedirá o exercício sob qualquer forma ou pretexto dos direitos dos titulares dos dados.

11º

1.O Segundo Outorgante, na qualidade de subcontratante, assume a responsabilidade pelo pagamento de quaisquer multas, sanções, indemnizações, danos e/ou prejuízos em que possa vir a ser condenado por factos que lhe sejam imputáveis no âmbito da utilização indevida dos Dados recolhidos e/ou tratados ao abrigo deste Acordo ou do Contrato.

2.É considerada utilização indevida dos Dados toda aquela que não for executada nos precisos termos das instruções dadas pelo Primeiro Outorgante.

Lisboa, Data

PRIMEIRO OUTORGANTE SEGUNDO OUTORGANTE

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Designação do Encarregado de Proteção de Dados

Considerando o disposto no Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados - RGPD) prevê, na alinea a) do nº 1 do artigo 37., que o responsável pelo tratamento designe um encarregado da proteção de dados sempre que o tratamento for efetuado por uma autoridade ou organismo público;

Assim, atento ao disposto supra, delibera a gerência da empresa nome da empresa lda. nomear XXXXXXXXXXX como EPD da empresa por um período de XX anos, período automaticamente renovável até que alguma das partes denuncie esta renovação

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.

Aviso de privacidade para recolha de dados

Os dados pessoais facultados à Empresa XXX pelos clientes destinam-se apenas ao cumprimento de contrato celebrado entre a Sociedade XXX e os clientes, podendo estes dados ser entregues aos Serviços Públicos e à autoridade judiciária por força de disposição legal. Nos termos da lei, os clientes podem solicitar, à Sociedade, o acesso ou retificação dos seus dados pessoais.

Disclaimer - Este é um modelo de documento que tem um caráter necessariamente genérico e que necessita de ser adaptado à realidade da organização.


COMPETE
2020


PORTUGAL
2020


UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional

Junho/2021