

## Pergunta 1.1

O 5º artigo do regulamento geral de proteção de dados, estipula que princípios e medidas deverão ser tomadas relativamente ao tratamento de dados pessoais.

Neste definem-se os dados pessoais dos titulares como objetos recolhidos sobre os utilizadores, de forma explícita e legítima, com finalidade transparente. Estes poderão ser atualizados, ou apagados, sempre que apresentem incoerências, e que o seu autor o pretenda, sendo que qualquer erro deverá ser retificado/apagado sem demora. Os dados poderão ainda ser guardados por períodos de tempo variáveis, de acordo com o estipulado pelo titular. Caso se tratem de arquivos de interesse público ou que requeiram investigação, poderão ser mantidos por maiores períodos de tempo. Fica ainda ao encargo da entidade responsável pela manutenção dos dados, quaisquer mecanismos que sejam necessários implementar para garantir a segurança destes mesmos dados (compreende perdas, danificação, destruição e tratamento não autorizado aos dados).

Tendo em conta todo o conteúdo do arquivo supracitado, pode-se determinar que um fator de extrema importância a ter em consideração no desenvolvimento de qualquer *software* que integre esta nova norma, será a segurança dos dados. Isto porque qualquer perda, ou interação ilícita dos dados, origina um processo onde a empresa responsável pelas informações sai gravemente lesada.

Para implementar mecanismos de segurança, poder-se-á recorrer numa fase inicial à minimização dos dados requeridos. Isto permite que apenas informação essencial seja guardada, diminuindo a preocupação de proteção de dados adicionais desnecessários. Dever-se-á sempre que possível, guardar metadados sobre a informação, por exemplo utilizando funções de *hash* criptográficas, aumentando a complexidade de obtenção de informações pessoais.

Outro mecanismo utilizado passará pela cifragem dos dados. Esta abordagem explícita diretamente uma forma de manter segurança de informação, garantindo que os dados apenas serão utilizados por entidades que tenham acesso a estes (evitando por conseguinte usos inadvertidos). Esta opção garante ainda que as entidades responsáveis pela manutenção dos dados terão, em caso de violação destes, apenas comunicar a autoridades de controlo (e não aos utilizadores per se).

Finalmente deverão ser implementadas ferramentas que inutilizem/neutralizem as informações pessoais dos utilizadores quando o período de tempo estipulado para permanência sobre responsabilidade das entidades termine. É imperativo que, apesar de remover os dados privados, as empresas garantam a integridade dos registos criados até à data.

Em suma, é importante desenvolver *software* seguro, que consiga apenas guardar o mínimo de informação possível, cifrada e preferencialmente metadados. Isto poderá, contudo, refletir-se numa diminuição da capacidade de interação entre os utilizadores e o *software* em si.