VIEIRA DE ALMEIDA

FLASH INFORMATIVO | FLASH NEWS

31 de janeiro de 2017

Magda Cocco | mpc@vda.pt
Inês Antas de Barros | iab@vda.pt
Isabel Ornelas | igo@vda.pt
Nádia Crujeira da Costa | ncc@vda.pt
Maria de Lurdes Gonçalves | mlg@vda.pt

PRIVACIDADE, PROTEÇÃO DE DADOS & CIBERSEGURANÇA

CNPD APROVA 10 MEDIDAS DE PREPARAÇÃO PARA A APLICAÇÃO DO REGULAMENTO EUROPEU SOBRE A PROTEÇÃO DE DADOS

A Comissão Nacional de Proteção de Dados ("CNPD") publicou, no passado dia 28 de Janeiro, um documento no qual estabelece 10 medidas para as organizações se prepararem para a aplicação do novo Regulamento Geral sobre a Proteção de Dados ("RGPD").

Uma vez que o RGPD será diretamente aplicável a partir de 25 de maio de 2018, a CNPD salienta que as entidades públicas e privadas deverão, desde já, implementar medidas e procedimentos internos para assegurar, até aquela data, o cumprimento das novas regras e obrigações.

A CNPD destaca 10 principais áreas de atuação, avançando com algumas ações a adotar pelas organizações, destacando-se as seguintes:

1. **Informação aos titulares dos dados**: atentas as novas regras do RGPD, todos os impressos, políticas de privacidade e demais textos informativos utilizados deverão ser revistos e reformulados de forma a incluir a informação adicional exigida pelo RGPD;
2. **Exercício dos direitos dos titulares dos dados:** as organizações deverão rever os procedimentos internos de resposta aos titulares dos dados, incluindo para efeitos do exercício dos novos direitos (desde logo, os direitos à portabilidade e ao esquecimento), por forma a garantir o cumprimento dos prazos e formalidades previstos no RGPD;
3. **Consentimento dos titulares dos dados**: as organizações deverão verificar a forma, as circunstâncias e os termos em que foi obtido o consentimento dos titulares dos dados e, caso não cumpram as novas exigências do RGPD, deverão obter novo consentimento;
4. **Dados sensíveis**: importa avaliar as categorias de dados pessoais tratados, de forma a identificar o eventual tratamento de dados sensíveis (categorias especiais de dados, nos termos do RGPD) e, assim, determinar os requisitos aplicáveis;
5. **Documentação e registo de atividades de tratamento:** as atividades relacionadas com o tratamento de dados pessoais devem ser documentadas, quer através da criação de um registo das atividades de tratamento de dados, quer através da implementação de outros procedimentos internos. Esta medida é essencial para que tanto as entidades responsáveis como as subcontratantes demonstrem o cumprimento do RGPD;

6. **Contratos de subcontratação:** os contratos celebrados com os subcontratantes deverão ser revistos, de forma a incluir um vasto conjunto de informações obrigatórias ao abrigo do RGPD. Por sua vez, e em caso de subcontratação pelos subcontratantes, estes deverão não só verificar os contratos celebrados, mas também confirmar que a sub-subcontratação foi autorizada pelos responsáveis pelo tratamento;
7. **Encarregado de proteção de dados:** para os casos em que o RGPD impõe a nomeação de um encarregado de proteção de dados (*Data Privacy Officer)*, as organizações devem, com antecedência, assegurar a existência desta figura, considerando o seu papel fulcral durante o período de implementação do RGPD. Mesmo nos casos em que esta nomeação não é obrigatória, a CNPD realça as suas vantagens para efeitos de garantir o cumprimento das obrigações do RGPD;
8. **Medidas técnicas e organizativas de segurança do tratamento:** as organizações deverão rever todas as políticas, práticas e medidas internas para confirmar um nível de segurança do tratamento adequado. As organizações deverão ainda implementar as medidas que se revelem necessárias para assegurar e poder comprovar o cumprimento do RGPD;
9. **Proteção de dados desde a conceção e avaliação de impacto**: importa avaliar o tipo de tratamentos de dados pessoais projetados, pelas organizações, para o futuro próximo, de modo a analisar a sua natureza e contexto, assim como os potenciais riscos para os titulares dos dados. Desta forma, as organizações garantem a aplicação dos princípios da proteção de dados desde a conceção e por defeito, conforme previsto no RGPD;
10. **Notificação de violações de segurança:** as organizações deverão adotar e implementar procedimentos internos de notificação de violações de segurança que envolvam dados pessoais. Estes procedimentos devem incluir regras e processos aplicáveis à deteção, identificação e investigação das circunstâncias da violação, medidas mitigadoras, fluxos de informação entre responsável e subcontratante, envolvimento do encarregado de proteção de dados e, quando aplicável, notificação à CNPD e aos titulares dos dados.

As organizações que ainda não iniciaram o processo de implementação do RGPD devem, o mais brevemente possível, rever e adaptar os seus procedimentos internos em matéria de proteção de dados pessoais, de forma a assegurar o cumprimento do RGPD até 25 de maio de 2018.

A CNPD continuará a divulgar orientações sobre o RGPD com vista a assegurar uma aplicação uniforme pelas organizações.

Este documento pode ser consultado em:

- https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf