



FÓRUM
GESTÃO DE DADOS
DE INVESTIGAÇÃO

Évora, 25 de novembro de 2022



Universidade do Minho

o papel dos encarregados da proteção de dados nos projetos de investigação

preocupações nas instituições de investigação e os desafios da abertura de dados.



Assuntos:

1. Dados abertos e Proteção de dados
2. O papel dos DPOs
3. Preocupações



1. Dados abertos e Proteção de dados



Dados abertos e Proteção de dados

O Princípio de Dados Abertos requer que os dados sejam disponibilizados em **ACESSO LIVRE** e disponíveis para **REUTILIZAÇÃO** posterior.

Tanto o **Acesso Livre** como a **Reutilização** (sem limites) são contrários ao espírito do regime de proteção de dados que determina que o **tratamento de dados pessoais** seja:

- o **MÍNIMO** necessário para finalidades **ESPECÍFICAS**

O RGPD determina especificamente, no artigo 25.º - “Proteção de dados desde a conceção e por defeito”, que “os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.”



Dados abertos e Proteção de dados

A **Reutilização** de dados pessoais está prevista, enquanto **exceção** no RGPD:

a) Apenas para **finalidades compatíveis** com as que justificaram a recolha original.

ou

b) Para **fins de investigação científica**, nesse caso sem o requisito de compatibilidade, mas com condições.

1. As Políticas de Dados Abertos não limitam o acesso e utilização a FINS CIENTÍFICOS...
2. Nenhum dos casos dispensa a Informação aos titulares e a determinação de uma Licitude para o tratamento posterior...



Dados abertos e Proteção de dados

Anonimização

A solução mais sólida e segura para este conflito, alinhada como o **Princípio da Minimização dos Dados**, será transformar os dados por forma a que deixem de ser dados pessoais, e já não se lhes aplique o RGPD.

A Anonimização é, de resto, um requisito do tratamento para fins de Investigação Científica:

“sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já **não permitam, a identificação dos titulares dos dados**, os referidos fins são atingidos desse modo.”

(RGPD, artigo 89.º, n.º.1 - Garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos)



Dados abertos e Proteção de dados

Requisitos para a Anonimização

- A **Anonimização** só será solução para Dados Abertos se for **EFETIVA**, isto é irreversível, qualidade que terá de ser garantida pelo Responsável pelo tratamento.
- A **Anonimização** não é um procedimento sem risco, é um compromisso entre a sua robustez e utilidade dos dados. A eficácia da **Anonimização** só pode ser verificada perante o conjunto concreto do dados.
- Há várias metodologias de **Anonimização**, que devem ser usadas consoante a natureza dos dados.
Ver documento “Opinion 05/2014 on Anonymisation Techniques”, WP216 do Article 29
- A anonimização pode ser comprometida com o passar do tempo e o surgimento de novos dados que quando cruzados com os primeiros possam levar à identificação dos titulares.

A anonimização (eficaz) é um grande desafio para os Dados Abertos e um risco para a Proteção de Dados.



Dados abertos e Proteção de dados

Acesso aos dados de forma controlada

Não são Dados Abertos, mas permitem **alguma Reutilização**.

Esta opção poderá ser necessária em situações em que a Anonimização é impossível, como em Estudos de Caso em que a informação de contexto é relevante e não permite esconder de forma eficaz a identidade dos participantes.

Esta solução tem **Impactos** para os titulares que devem ser identificados e tratados



Dados abertos e Proteção de dados

Acesso aos dados de forma controlada

Algumas medidas para mitigar os Impactos:

- Conceder acesso apenas para finalidades dentro de um domínio limitado de investigação, previamente autorizado pelo titular;
- Intermediar o consentimento a dar pelos Titulares ao novo Responsável e suas finalidades;
- Manter um registo dos Destinatários dos dados.

A solução concreta deverá ser alvo de avaliação Ética e de Impacto quanto à proteção de dados.



Dados abertos e Proteção de dados

O novo **Digital Governance Act** prevê a figura de **Altruísmo de Dados** com o intuito viabilizar a reutilização de dados pessoais para fins de interesse comum/geral:

«**Altruísmo de dados**», a partilha voluntária de dados, com base no consentimento dos titulares dos dados para o tratamento dos respetivos dados pessoais (...) para **fins de interesse geral**, previstos no direito nacional, se aplicável, tais como os **cuidados de saúde**, a **luta contra as alterações climáticas**, a **melhoria da mobilidade**, a **facilitação do desenvolvimento**, **produção e divulgação de estatísticas oficiais**, a **melhoria da prestação dos serviços públicos**, a **elaboração de políticas públicas** ou a **investigação científica de interesse geral**;

O Altruísmo de Dados é concretizado por meio de Organizações de Altruísmo de Dados que gerem os direitos dos titulares junto destes e dos Destinatários dos Dados.

Veremos como este conceito se materializa...



Dados abertos e Proteção de dados

Outras tensões entre Dados Abertos e Proteção de Dados

- Licitude para o tratamento posterior dos dados pessoais
 - O consentimento obtido originalmente deverá ser específico, o RGPD não prevê consentimentos que autorizem toda e qualquer finalidade.
 - O consentimento obtido pelo primeiro Responsável não serve para os seguintes.
 - Outras licitudes é complicado...
- Transferência de dados para países terceiros sem garantias quanto à proteção de dados
 - Acessibilidade dos dados a partir de jurisdições sem regime de proteção de dados, ou regimes não conformes com o padrão da UE
- Irrevogabilidade das Licenças CC
 - Após o acesso a um trabalho ou a conjunto de dados com uma determinada licença, o beneficiário terá permanentemente o direito à sua reutilização, nos termos dessa licença, ainda que esta seja posteriormente alterada.
 - Os titulares dos dados têm direito a retirar o consentimento para o tratamento dos seus dados, sem apresentar motivo, e direito a solicitar a sua eliminação.



2. O papel dos Encarregados da Proteção de Dados



O papel dos Encarregados da Proteção de Dados

Artigo 39.º - Funções do encarregado da proteção de dados (DPO)

- **Informa e aconselha** o Responsável pelo tratamento a respeito das suas obrigações nos termos do presente regulamento (RGPD) e de outras disposições de proteção de dados da União ou dos Estados-Membros;
- Presta aconselhamento, quando tal lhe for solicitado, no que respeita à **avaliação de impacto sobre a proteção de dados** e controla a sua realização nos termos do artigo 35.º;

Artigo 35.º - Avaliação de impacto sobre a proteção de dados

- Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o **parecer do encarregado da proteção de dados**, nos casos em que este tenha sido designado.



O papel dos Encarregados da Proteção de Dados

- Os investigadores enquanto Responsáveis pelo tratamento têm no DPO um especialista que lhes dará orientações sobre a conformidade do seu projeto quanto ao tratamento de dados pessoais.
- Os pareceres do DPO, além da utilidade dos seus contributos... serão demonstração da diligência do Responsável quanto à Proteção de Dados.
- O “custo” de consultar o DPO será:
 - A tarefa de o consultar, pois será necessário descrever-lhe o tratamento nos termos que o DPO pedir.
 - O risco do DPO recomendar a realização de uma Avaliação de Impacto sobre a Proteção de dados.
 - O parecer do DPO poderá levar a alterações nos tratamentos, eventualmente limitações, mas cabe ao Responsável decidir o que será razoável e o que será excessivo.



O papel dos Encarregados da Proteção de Dados

- Na UMinho os trabalhos de investigação com humanos estão sujeitos a parecer do Conselho de Ética, que também se pronuncia sobre a conformidade do tratamento de dados pessoais. Não é regra o parecer do DPO.
- O parecer do DPO da UMinho pode ser pedido preenchendo um formulário de Registo de tratamentos de dados pessoais. Esse formulário inclui um teste à necessidade de realizar uma AIPD de acordo com os critérios da CNPD e do Grupo do Artigo 29/Comité Europeu da Proteção de Dados.
“Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679”, WP248
- Na página Web da Proteção de dados é disponibilizado também um modelo de Avaliação de Impacto.



O papel dos Encarregados da Proteção de Dados

- **Notificação de violações de dados pessoais na UMinho**
 - As violações de dados pessoais são comunicadas pelos Responsáveis ao DPO para registo e avaliação das medidas a tomar para proteção dos titulares dos dados pessoais, nomeadamente a notificação da Autoridade de Controlo ou dos Titulares dos dados.
 - A comunicação ao DPO faz-se por meio do formulário disponível na página da Proteção de dados da UMinho



O papel dos Encarregados da Proteção de Dados

- Intermediação entre os titulares e o Responsável do tratamento
 - O contacto do DPO deverá fazer sempre parte das informações prestadas aos titulares.
 - O DPO sendo único, será mais fácil de encontrar que cada Responsável por projetos de investigação.



3. Preocupações



Preocupações

Adequação dos recursos utilizados para alojamento de dados de investigação

- As instituições de investigação devem prover os recursos necessários à investigação de forma centralizada, para que se adquiram **soluções com capacidades, suporte e administração de nível institucional** e não de nível pessoal ou de grupo de trabalho.

Sem soluções institucionais, cada projeto resolverá o seu problema, de acordo com a sua sensibilidade para o assunto, criando-se a oportunidade para soluções de alojamento inadequadas como:

- discos externos sem devidas proteções contra danos físicos ou extravio;
- serviço na nuvem sem contrato, ou com contrato inadequado à proteção dos dados.
- serviço na nuvem em países sem garantias adequadas quanto ao acesso pelas autoridades.
- dispositivos de utilização pessoal, sujeitos a riscos dessa natureza de utilização.
- ...



Preocupações

Segurança da informação

A atividade criminosa online tem aumentado muito, ninguém parece estar a salvo.

É muito importante:

- O cumprimento individual de boas práticas de segurança informática.
- A pseudonimização dos dados, com o isolamento dos dados de identificação em dispositivo diferente, sujeito a especiais medidas de segurança e restrição de acessos.
- A utilização de software legítimo, com suporte do fabricante e em dia quanto a atualizações de segurança.
- A proteção do conjunto, rede e dispositivos, com ferramentas de natureza transversal à instituição, como gestão centralizada e especializada, para uma visão global da instituição. *(todos precisam, mas quem é que paga?)*



Preocupações

Publicação de dados identificáveis em repositórios de dados abertos

- Falta de consciência da inadequação da publicação de dados identificáveis;
- ... mesmo daqueles que tenham sido obtidos publicamente.
- Falta de consciência dos desafios para alcançar uma anonimização efetiva
 - e a subtiliza da classificação de dados como “identificáveis”.
- Complexidade e volume dos dados dificultam a sua sanitização.
- O risco de identificação acrescido pela informação nos Metadados.
- Natureza autónoma e responsabilidade individual da publicação de dados em repositórios de dados



Universidade do Minho

Obrigado

Jorge Figueiredo
jorgef@reitoria.uminho.pt