A Ciência Aberta é possível com dados clínicos? Ferramentas para planeamento e avaliação de risco

Joana Rodrigues, Célia M. D. Sales, Paula Mena Matos, João Aguiar Castro, Cristina Ribeiro

INESC TEC, FEUP, FPCEUP, Universidade do Porto

16 de novembro de 2018

25 de maio de 2018

RGPD

Regulamento Geral de Proteção de Dados


Transparência


Lei


Políticas


Requisitos


Governança


Normas


Regulamentos


Regras

Mudança do paradigma

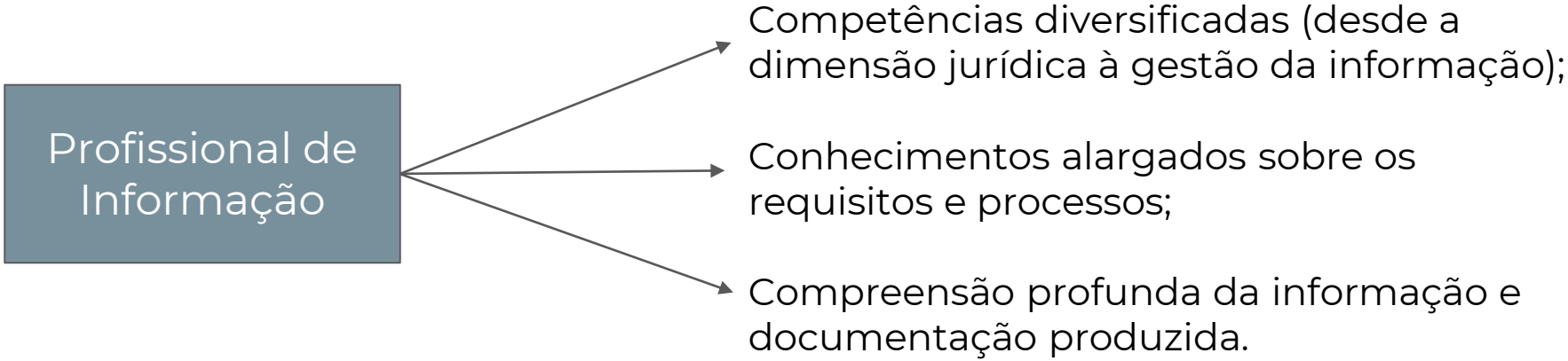
Cidadão tem o controlo total sobre os seus dados pessoais (consentimento)

Adaptação do mercado e da sociedade à economia digital

A heteroregulação dá lugar à autoresponsabilização das organizações

CNPD como autoridade nacional de controlo

RGPD na ótica do PI



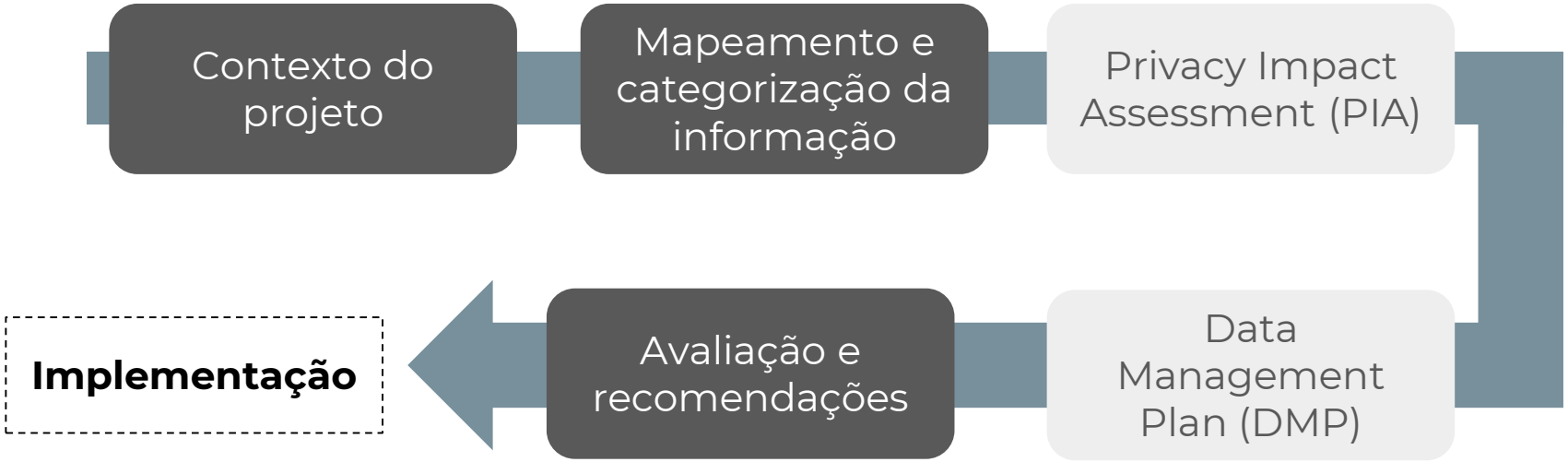
RGPD no âmbito da Gestão de Dados

Segundo a Comissão Europeia, os dados que requerem prudência no seu tratamento por serem considerados sensíveis são:

- Dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas;
- Filiação sindical;
- Dados relativos à vida sexual ou orientação sexual da pessoa;
- Dados genéticos, dados biométricos tratados para identificar um ser humano;
- **Dados relacionados com a saúde.**

Tendo em conta estas circunstâncias, como devem lidar os investigadores produtores desta tipologia de dados para assegurar as políticas apontadas pela Ciência Aberta?

Fluxo de trabalho



Privacy Impact Assessment (PIA)

Como avaliar e monitorizar o impacto de dados pessoais?

- Avaliar os riscos sobre a tecnologia
- Avaliar os riscos sobre os processos
- Estabelecer medidas para minimizar os riscos
- Resolver problemas

Data Management Plan (DMP)

Como cumprir as políticas de Acesso Aberto?

Especificar como os dados são:

- Recolhidos
- Documentados
- Organizados
- Disponibilizados
- Preservados

Projeto TOGETHER

Estudo de caso no campo da Psico-Oncologia

ref. NORTE-01-0145-FEDER-030980

U.PORTO
FACULDADE DE PSICOLOGIA E DE CIÊNCIAS DA EDUCAÇÃO UNIVERSIDADE DO PORTO

IPOPORTO
INSTITUTO PORTUGUÊS DE ONCOLOGIA DO PORTO FG, EPE

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

PIA TOGETHER

Tabela 1) Avaliação e plano de minimização dos riscos de privacidade e da qualidade dos dados

RISCOS	MEDIDAS
Identificação dos participantes através do seu nome	• Anonimização dos questionários e das bases de dados, através de código de identificação; • A correspondência entre o nome dos participantes e o seu código será apenas do conhecimento do elemento da equipa responsável pela sua construção, o PI e Co-PI; • Esta informação ficará na posse exclusiva do PI e Co-PI, armazenada da forma mais segura possível.
Dispersão ou perda de questionários em papel respondidos pelos participantes	• Arquivo dos questionários em papel em local fechado, à guarda do PI e Co-PI, com acesso restrito aos elementos da equipa envolvidos no seu tratamento; • Cinco anos após o final do projecto, destruição dos questionários em papel.

RISCOS	MEDIDAS
Perda de informação de contexto dos dados (quando são recolhidos, tratados, em que condições, por quem, etc)	• Escolha de modelo de metadados, com consultoria de equipa especializada da FEUP; • Formação dos membros da equipa em boas práticas de gestão de dados; • Membro da equipa que recolhe dados fica com a responsabilidade de garantir registo de metadados no momento da recolha e no armazenamento dos dados.
Perda e danos de equipamento (portátil, disco rígido), ou perda de dados no equipamento	• Armazenamento dos dados num servidor restrito, apenas acessível aos elementos do projecto, que agrega todos os dados e que permite uma colaboração online; • Backup periódico em disco rígido externo encriptado.
Dispersão de ficheiros de dados em equipamentos de diversos membros da equipa	• Agregação de todos os dados no servidor .
Perda de ligação online que comprometa acesso ao servidor	• Backup periódico em disco rígido externo, com informação encriptada.
Preservação dos ficheiros de dados	• Os ficheiros de som serão apagados após validação da sua transcrição; • Os ficheiros com outros tipos de dados serão mantidos apenas o tempo necessário para a sua utilização.

RISCOS	MEDIDAS
Perda de controle do uso dos dados	• Política de acesso ao servidor, com autenticação e diferentes níveis de permissão de acesso aos conteúdos, de acordo com o necessário para a execução das tarefas do projecto; • Para além dos elementos que tratam os dados, apenas o PI e CO-PI têm acesso total aos dados do servidor; • Disco rígido de backup com acesso restrito ao elemento do projecto responsável pelo backup, assim como ao PI e CO-PI; • Findo o projecto, o acesso aos dados no servidor fica restrito aos administradores (PI e CO-PI) e o disco rígido de backup fica à guarda do PI e Co-PI; • Todos os elementos externos ao projecto que prestem serviços relacionados com o tratamento de dados, assinam acordo de confidencialidade.
Falha de segurança no processo de comunicação de dados entre membros da equipa	• Reduzir ao máximo o uso do mail para partilha de dados, usando prioritariamente o servidor; • No caso de ser indispensável o envio por email, os ficheiros deverão seguir em formato protegido.
Não cumprimento do plano de gestão de dados	• Até três meses após o início do projecto, estará elaborado um plano detalhado com as melhores soluções técnicas para a implementação das presentes medidas; • O cumprimento deste plano será periodicamente verificado por um terceiro e reportado anualmente no relatório de actividade do projecto.

Trabalho futuro

- Sistematização do levantamento de requisitos efetuado;
- Modelação de processos;
- Revisão do PIA;
- Elaboração do DMP;
- Nova avaliação da documentação produzida pela Comissão de Ética do IPO;
- Acompanhamento dos investigadores do projeto nas atividades de gestão de dados de investigação.