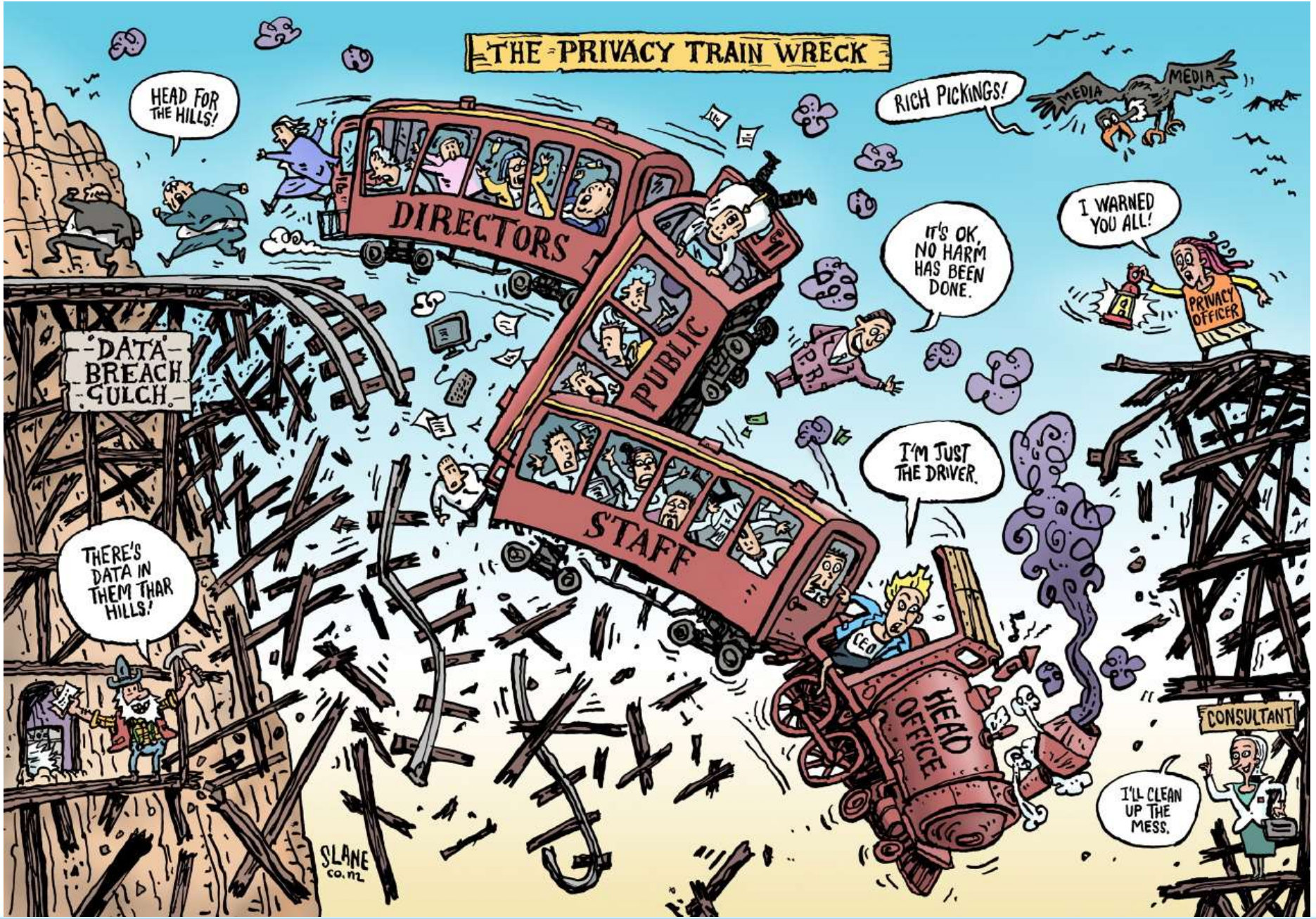
LOCAL GOV 4.0 TALKS

O VALOR DO DIGITAL
NA GESTÃO PÚBLICA LOCAL

PRIVACY BY DESIGN

Beatriz Bagoin Guimarães – CIPP/E


THE PRIVACY TRAIN WRECK
HEAD FOR THE HILLS!
DIRECTORS
PUBLIC
STAFF
DATA BREACH GULCH
THERE'S DATA IN THEM THAR HILLS!
RICH PICKINGS!
MEDIA
MEDIA
IT'S OK, NO HARM HAS BEEN DONE.
I WARNED YOU ALL!
PRIVACY OFFICER
I'M JUST THE DRIVER.
CEO
HEAD OFFICE
CONSULTANT
I'LL CLEAN UP THE MESS.
SLANE CO.NZ

LOCAL GOV 4.0 TALKS

O VALOR DO DIGITAL
NA GESTÃO PÚBLICA LOCAL

Pré-GDPR

Contexto

- Não se trata de um conceito novo
- A *framework* base foi desenvolvida nos anos 90 e começou a ser generalizada em 2010
- Ann Cavoukian, Information and Privacy Commissioner em Ontario, Canadá definiu 7 princípios base

Princípios base

1. Proactivo e não reactivo. Preventivo e não correctivo

O objectivo é sempre antecipar os eventos e os riscos antes que ocorram e evitar que sem venham a concretizar.

2. *Privacy by default*

Os dados devem estar automaticamente protegidos nos sistemas e nos processos sem necessidade de acção por parte dos indivíduos.

Princípios base

3. *Privacy by design*

A privacidade é uma componente essencial do sistema sendo embebida nos processos de planeamento e desenvolvimento e acompanhando todas as etapas.

4. Funcionalidade global

O objectivo é equilibrar os legítimos interesses e objectivos com a privacidade de forma a atingir uma situação de "*win-win*".

Princípios base

5. Ciclo de vida completo

A privacidade faz parte do processo desde o início até ao fim do ciclo de vida da informação, assegurando a sua destruição de acordo com os prazos previstos.

6. Visibilidade e transparência

O objectivo é assegurar todos os *stakeholders* de que estão ser considerados todos os objectivos e premissas e que isso pode ser verificado de forma independente.

Princípios base

7. Respeito pela privacidade do indivíduo

As funcionalidades são implementadas tendo sempre como prioridade a privacidade do indivíduo usando mecanismos de *privacy by default*, notificações e opções *user-friendly*.

LOCAL GOV 4.0 TALKS

O VALOR DO DIGITAL
NA GESTÃO PÚBLICA LOCAL

GDPR

GDPR

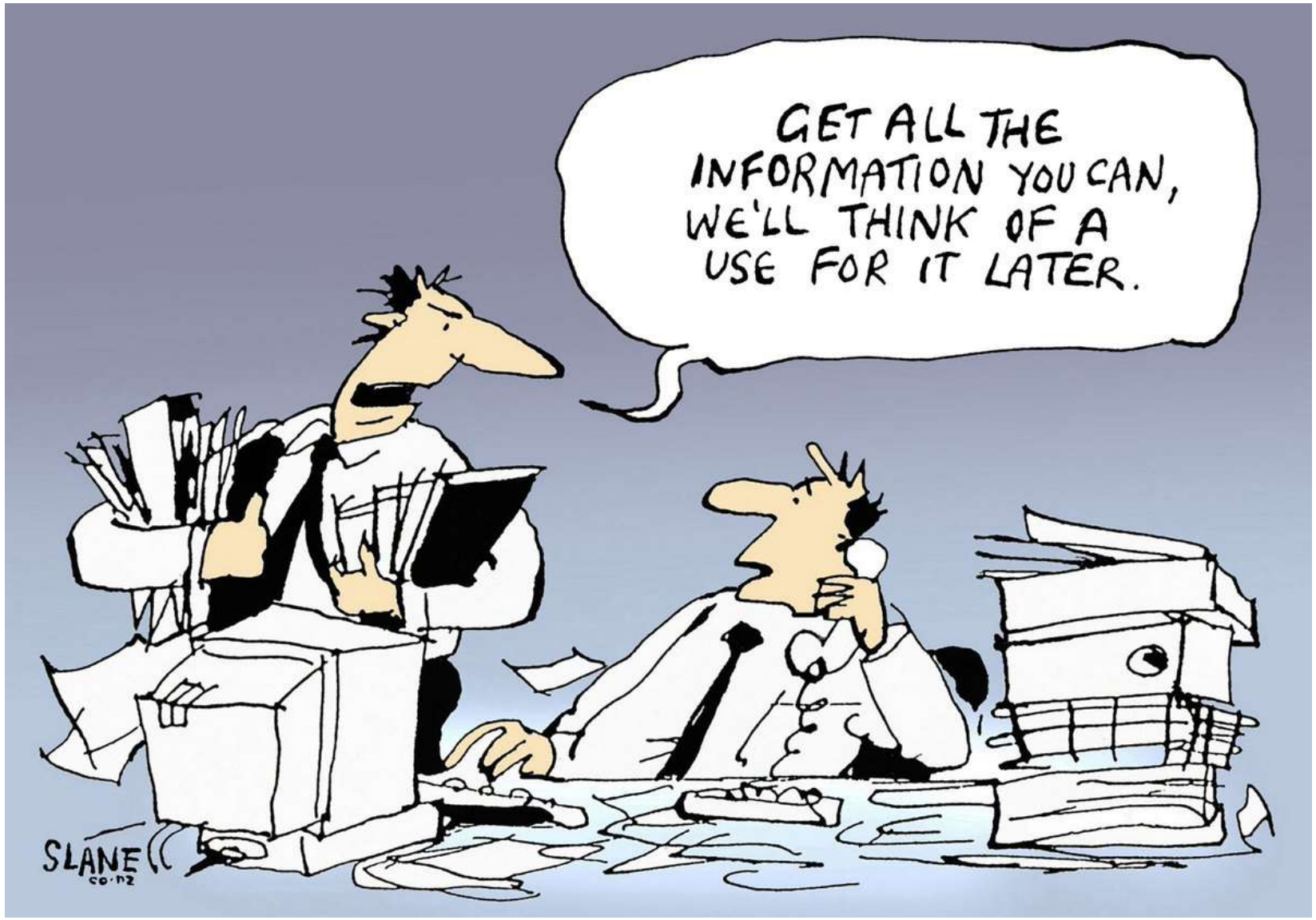
Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os **princípios da proteção de dados desde a conceção e da proteção de dados por defeito**. Tais medidas podem incluir a **minimização do tratamento de dados pessoais**, a **pseudonimização** de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, **haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção** e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. **Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos**. **(Considerando 78)**

GDPR

Artigo 25º - Proteção de dados desde a conceção e por defeito

1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as **medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização**, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.

2. O responsável pelo tratamento aplica medidas técnicas e organizativas **para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade especifica do tratamento**. Essa obrigação aplica-se a **quantidade** de dados pessoais recolhidos, a **extensão** do seu tratamento, ao seu **prazo de conservação** e a sua **acessibilidade**. Em especial, essas medidas asseguram que, por defeito, os dados pessoais **não sejam disponibilizados sem intervenção humana a um numero indeterminado de pessoas singulares**.


GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
SLANE co.nz

Privacy by design

- O ciclo de desenvolvimento de sistemas tem que incluir preocupações relativas à protecção dos dados e direitos dos titulares de dados **desde o início**
- Torna-se muito mais difícil assegurar estas salvaguardas em etapas posteriores
- Este conceito não se restringe apenas à concepção de produtos, mas deve **abranger também a concepção de procedimentos**
- Devem ser garantidos procedimentos de gestão de risco e avaliação de produto/procedimento que **mitigam esses riscos** durante o processo de desenvolvimento

Privacy by design

- É necessário garantir que são recolhidos os dados exactamente **necessários e legítimos** em cada ocasião
- Devem ser tratados os dados apenas para o **propósito** inicial definido, **dentro do prazo** previsto e **regras de conservação**
- O **acesso** aos dados pessoais deve ser restringido de acordo com as **necessidades de perfil** de cada membro da equipa

Medidas a implementar

- **Mapeamento e classificação e organização dos dados pessoais** de forma a garantir uma resposta eficiente às autoridades de controlo e titulares de dados
- Configuração dos sistemas para despoletarem automaticamente os **mecanismos de eliminação** de dados pessoais nos prazos previstos
- Desenho de formulários para recolher os **dados estritamente necessários**
- **Pseudonimização** dos dados quando tal for possível
- Configuração de mecanismo para **isolar e facilmente eliminar os dados de titulares** que não pretendam receber mensagens de marketing
- Estruturação de dados em **formatos interoperáveis** de forma a garantir os requisitos de portabilidade

Documentos de apoio

Regulamento Geral de Protecção de Dados – Parlamento Europeu e Conselho

https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Privacy by Design in Law, Policy and Practice - Ann Cavoukian

https://gpsbydesign.org/privacy-by-design-in-law-policy-and-practice-a-white-paper-for-regulators-decision-makers-and-policy-makers/

Pseudonymisation techniques and best practices – ENISA
https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

Anonymisation Techniques – WP29

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

LOCAL GOV 4.0

O VALOR DO DIGITAL
NA GESTÃO PÚBLICA LOCAL

Obrigada

Beatriz Bagoin Guimarães

bguimaraes@quidgest.com

Quidgest APDSI CIO GESBANHA PH INFORMATICA saphety