GDPR E O WHOIS DEPOIS DE AMANHÃ

RUBENS KÜHL
GTS 31 – 23.05.2018

Produto x Jurídico


Why are you sending me all these emails asking me if I want more emails?


It's because of GDPR

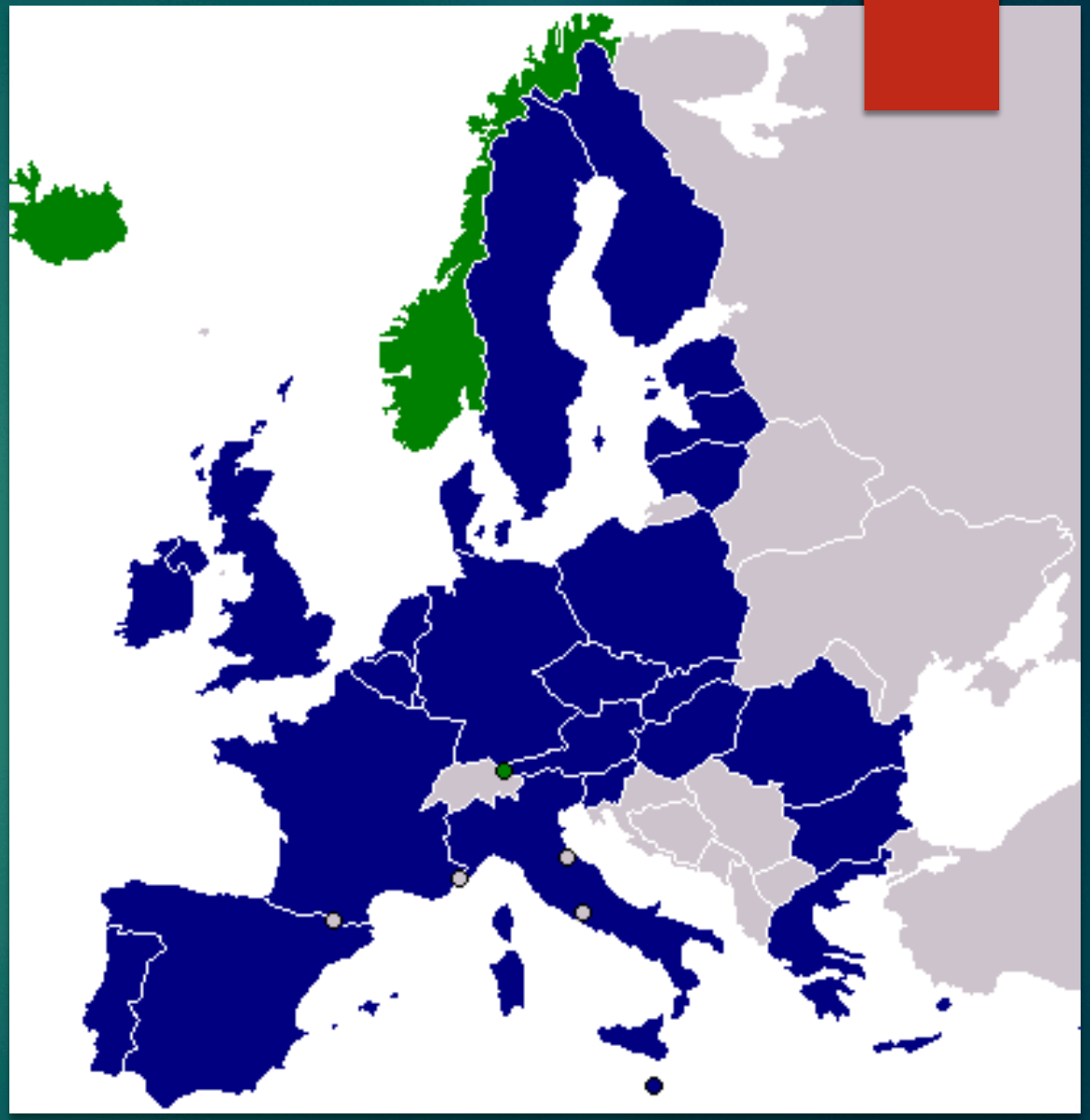

But GDPR is supposed to mean fewer emails!


You are a valued customer!


UNSUBSCRIBE!
imgflip.com

GDPR

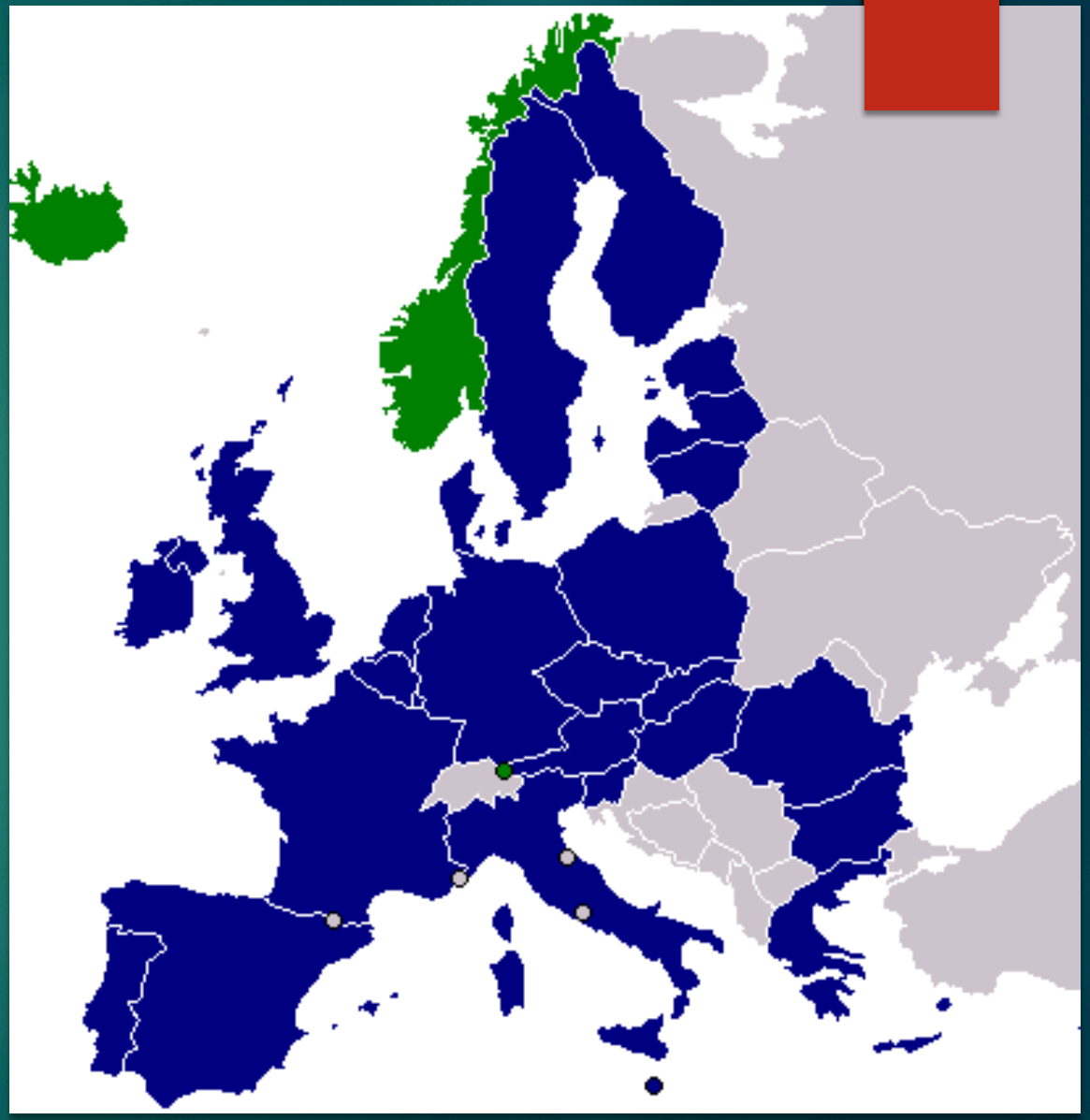
- O que é ?
- Onde vive ?
- Do que se alimenta ?



Linha do tempo da GDPR

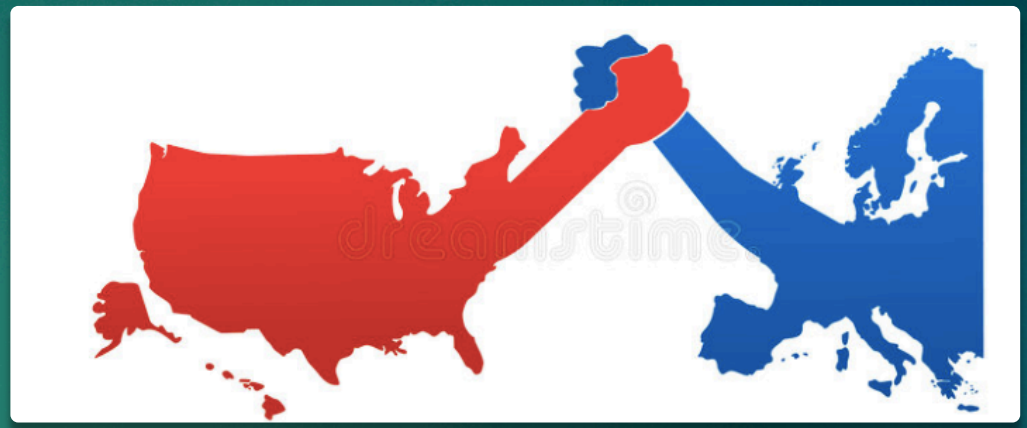
GDPR

- O que é ?
- Onde vive ?
- Do que se alimenta ?



GDPR

- O que é ?
- Onde vive ?
- Do que se alimenta ?



E o “kiko” ?

- Você está no EEE ?
- Você oferece serviços para residentes no EEE ?
- Você monitora comportamento de residentes no EEE ?
- Você usa serviços de empresas européias ?

Então é só olhar o IP e…

- Um residente no EEE…
  - … pode estar a passeio em outros países ao realizar transações
  - … pode ter cartão de crédito de outros países
  - … pode trabalhar para uma empresa estrangeira que exige navegação via proxy corporativo
  - … pode ter e-mail @serviço.ccTLD
  - … pode não ter passaporte do EEE
- … e geolocalização #fail.

Dados pessoais

- Toda informação relacionada a uma pessoa natural que pode ser usada para direta ou indiretamente identificar tal pessoa
- Inclui
  - Nome
  - Foto
  - E-mail
  - Dados bancários
  - Postagens em redes sociais
  - Informações de saúde
  - Endereços IP

Princípios

- Concepção orientada à privacidade
- Legalidade, equidade e transparência
- Limitação de propósito
- Minimização de dados
- Exatidão
- Armazenamento transitório
- Integridade e confidencialidade
- Responsabilidade

Parêntese: Responsabilidade em casos de vazamento de dados pessoais

Consentimento na GDPR

- Itemizado
- Linguagem clara e acessível
- Revogável
- Necessário para o serviço

Controlador e Processador

- Um controlador determina porque dados são processados
- Um processador armazena ou processa dados para terceiros
- Uma organização pode ter os dois papéis
- Mais de uma organização pode controlar um processo, mas todas são imputáveis

Parêntese: Brasil

- Na questão de legalidade, o artigo 6, (1)c diz "... o processamento é necessário para cumprir uma obrigação legal a que o controlador esteja sujeito"
- A CF/88 diz (art. 5º,IV) "é livre a manifestação do pensamento, sendo vedado o anonimato."
- Assim, controladores brasileiros e controladores estrangeiros lidando com dados de brasileiros precisam, para estar em conformidade com a GDPR e a legislação brasileira, identificar propriamente tais manifestações.

WHOIS de gTLDs após a GDPR

- Não mais mostrados:
  - Nome
  - E-mail
  - Telefone
  - Endereço
  - Cidade
  - Contatos administrativo, técnico e cobrança
- *Registrars* proverão formulário de contato ou equivalente

```
Domain Name: nic.app
Registry Domain ID: 6D67D1-APP
Registrar WHOIS Server: whois.nic.google
Registrar URL:
Updated Date: 2015-10-02T19:40:59Z
Creation Date: 2015-06-22T20:34:34Z
Registry Expiry Date: 2018-06-22T20:34:34Z
Registrar: Charleston Road Registry NonBillable
Registrar IANA ID: 9999
Domain Status: ok https://icann.org/epp#ok
Registrant Organization: Charleston Road Registry, I
Registrant State/Province: CA
Registrant Country: US
Name Server: ns1.google.com
Name Server: ns2.google.com
Name Server: ns3.google.com
Name Server: ns4.google.com
DNSSEC: unsigned
```

Mais detalhes desse novo WHOIS

- Se aplica
  - Ou a indivíduos do EEE, ou a tudo, a critério do *registry / registrar*.
  - A dados de pessoa física ou a tudo, a critério do *registry / registrar*.
- Acesso a dados completos
  - Permitido inicialmente por solicitação específica (granular)
  - Futuramente por modelo de certificação (ainda incerto se granular ou em larga escala)
  - Receptor dos dados passa a ser obrigado a seguir GDPR no seu processamento
- Publicação completa poderá ser solicitada pelo indivíduo
  - Suporte a esse recurso provavelmente não disponível no dia 25
- Previsão de implantação mandatória de RDAP até meados de Novembro

E agora, como fazer com investigações de segurança ?

”Para quem eu reclamo ?”

- Contatos de abuse do *registrar* continuam sendo mostrados
- Alguns *registrars* mostram quem vendeu (*reseller*)
- WHOIS de IPs indicando provedor de hospedagem também não (ou pouco) afetados
- E-mail no SOA do domínio
- E-mail no SOA do DNS reverso
- E-mail no *site*

“Este é um domínio legítimo ou sacanagem ?”

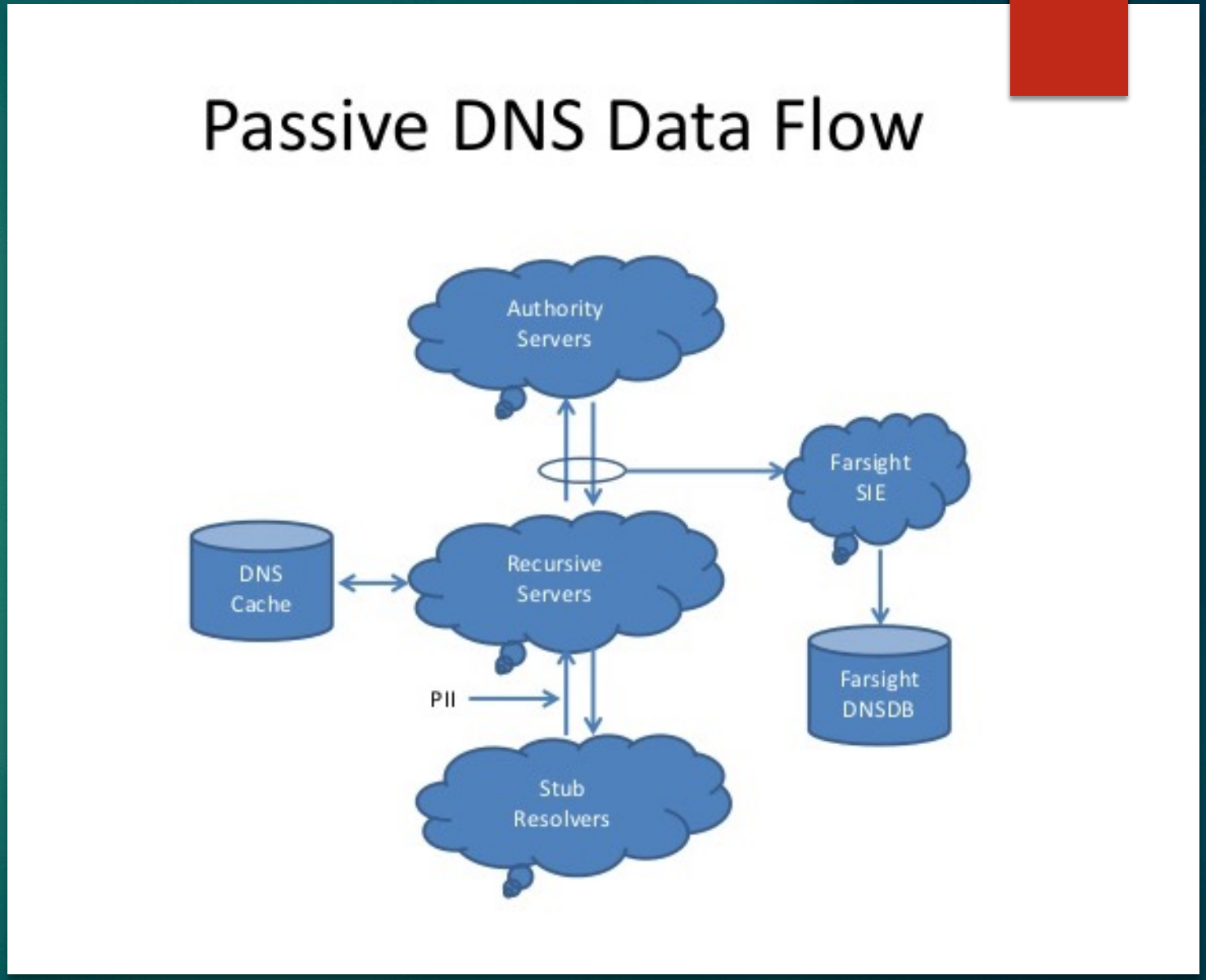
- Esta era uma pergunta simples de responder...
- Agora, boas práticas podem incluir configuração de servidores DNS no domínio e de resposta autoritativa em servidores DNS para
  - Exemplo: grandebanco.TLD

    ```
    Nameserver: propriedadeintelectual1.grandebanco.com.br
    Nameserver: propriedadeintelectual2.grandebanco.com.br
    ```

  - E, claro, solicitar publicação dos dados assim que o *registrar* e o *registry* suportarem (inclusive considerando mudar para um *registrar* que esteja mais adiantado nessa implementação)

“Descobri um abuso. Que outros existem ?”

- Apesar de não mais correlacionável diretamente, é possível denunciar ao registry / registrar que poderá fazer essa correlação com os dados não publicados.
- É possível também correlacionar por DNS passivo, que já é usado como fonte significativa de inteligência sobre abusos empregando DNS



Proposta de recuperação de capacidade de correlação

- Introduzida por Jonathan Matkowsky (RiskIQ)
- Consiste de inserir nos dados públicos chaves que permitem correlacionar domínios entre diferentes registrars e registries
- Exemplo:

```
Registrant Name Hash: 29FD2EA9
Registrant Email Hash: 37BC671231
```

- Além de aplicações de segurança, pode ser útil também para propriedade intelectual (ex: estabelecer padrões de *cybersquatting*)
- Incerto se será incorporado pela ICANN e se terá autorização das autoridades europeias de privacidade
- Método de transformação (*hash*, *salt*, iterações, chave pública/ privada, filtro Bloom, estático x variável etc.) ainda precisa ser pensado para evitar obsolescência precoce do processo.

Para mais informações, ligue…

https://gdprchecklist.io/

http://gdpr.ninja/

https://www.eugdpr.org/

https://iapp.org/

https://gdpr-info.eu

Obrigado!

Rubens Kühl
nome mais primeira letra do sobrenome @ gmail.com