SUCESU-RS

Grupo de Usuários de Segurança - GUSEG

Conhecendo a GDPR e a LGPD sob o olhar de Segurança da Informação

Paulo Rogério Dias de Oliveira

GU Segurança

SUCESU-RS
Associação dos Usuários de Informática e Telecomunicações do RS

Agenda do Dia

- 19:45 - Abertura
- 20:00 – Titulo
- 21:00 - Perguntas
- 21:15 - Coffee-End

GU Segurança

Tópicos

- Breve Resumo GDPR e LGPD
- Tipos de processamento de dados
- Requisitos da Aplicação
- Dados Pessoais
- Controlador e Operador
- Consentimento
- Direitos dos titulares dos dados
- Notificação de Incidentes
- Sanções
- Principais área impactadas
- Responsável pela proteção de dados – DPO / APD
- Conceito – Privacy by design
- O que fazer para ficar compliance?

GU Segurança

Resumo LGPD - GDPR

LGPD

- Lei n.° 53/2018 aprovada em Agosto/18
- Passa a valer em Fevereiro/2020

GDPR

- Aprovada em Abril/2019
- Em vigor desde Maio/2018

GU Segurança

Tipos de processamento de dados relevantes pelas regulamentações

Tipos de processamento de dados considerados pelas regulamentações ...

- Coleta
- Produção
- Recepção
- Classificação
- Utilização
- Acesso
- Reprodução
- Transmissão
- Distribuição
- Processamento
- Arquivamento
- Armazenamento
- Eliminação
- Avaliação ou Controle da Informação
- Modificação
- Comunicação
- Transferência
- Difusão
- Extração

… de dados

GU Segurança

Requisitos da Aplicação

GDPR

Qualquer operação que tenha por objetivo ofertar bens ou serviços ao **mercado Europeu**

Tratamento de dados de indivíduos Europeus ou **Residentes** na UE, quando da oferta de produto ou serviços a indivíduos situados na UE

LGPD

Para qualquer operação que tenha por objetivo ofertar bens ou serviços ao **mercado Brasileiro**

Para coleta e tratamento de dados pessoais realizado dentro ou fora do Brasil, desde que os dados tenham sido coletados aqui.

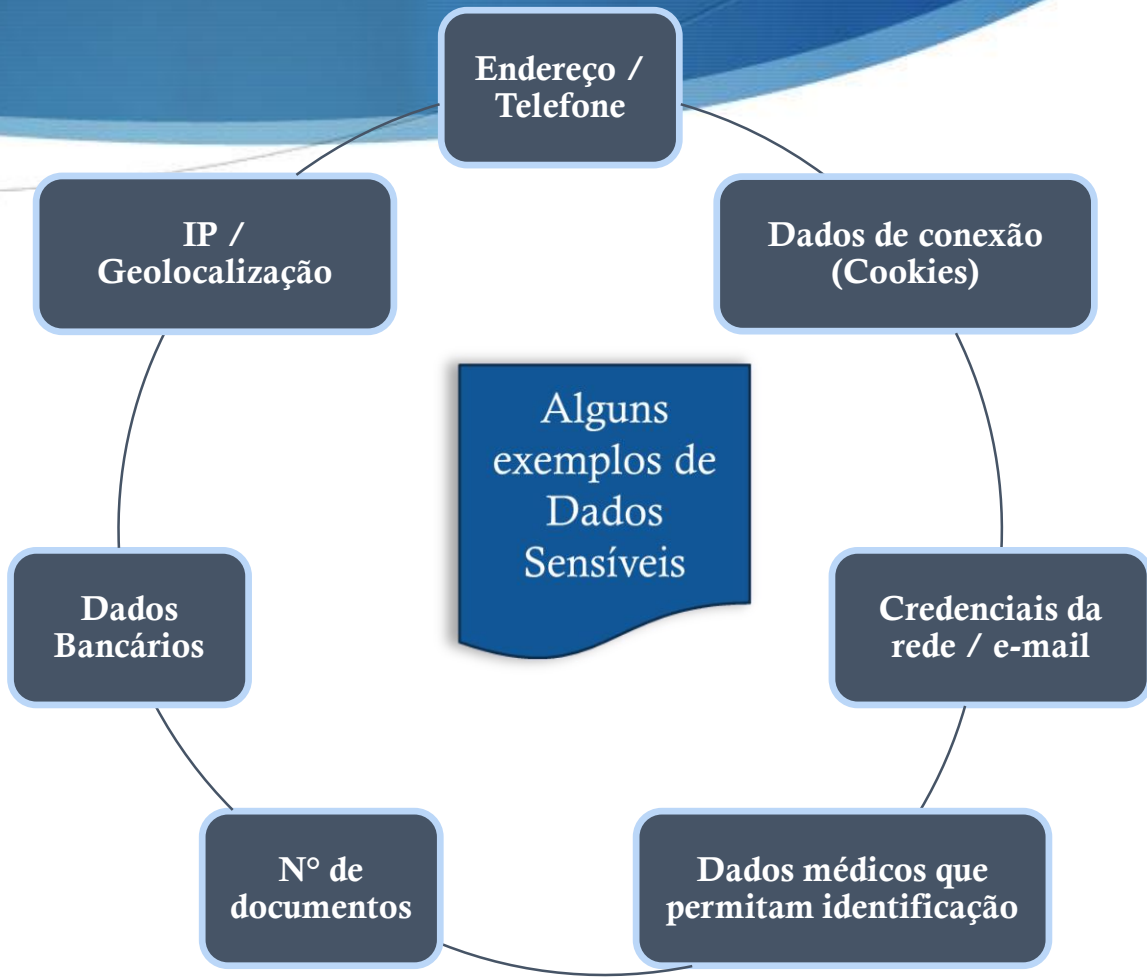
GU Segurança

Dados Pessoais

<u>Dado Pessoal</u> é qualquer informação, que a identifica diretamente ou a torna identificável.

Ex:

Paulo + Oliveira + @sicredi



GU Segurança

Controlador e Operador

Controlador: Organização ou individuo que **determina** como os dados pessoais serão tratados.
Ex: Banco

Operador: Organização ou indivíduo que **processa** os dados pessoais por ordem do controlador.
Ex: Serviço de nuvem contratado.

Agentes de Tratamento

Responsabilidade Solidária

A GDPR e a LGPD estabelecem que ambos serão diretamente sujeitos a lei ainda que o controlador tenha mais obrigações regulatórias.

GU Segurança

Consentimento

<u>Consentimento</u> deve ser uma manifestação de vontade específica, clara, dada livremente pelo individuo.

Deve:

- Informado / Específico
- Ser documentado para evidência
- Ter a opção de ser facilmente retirado

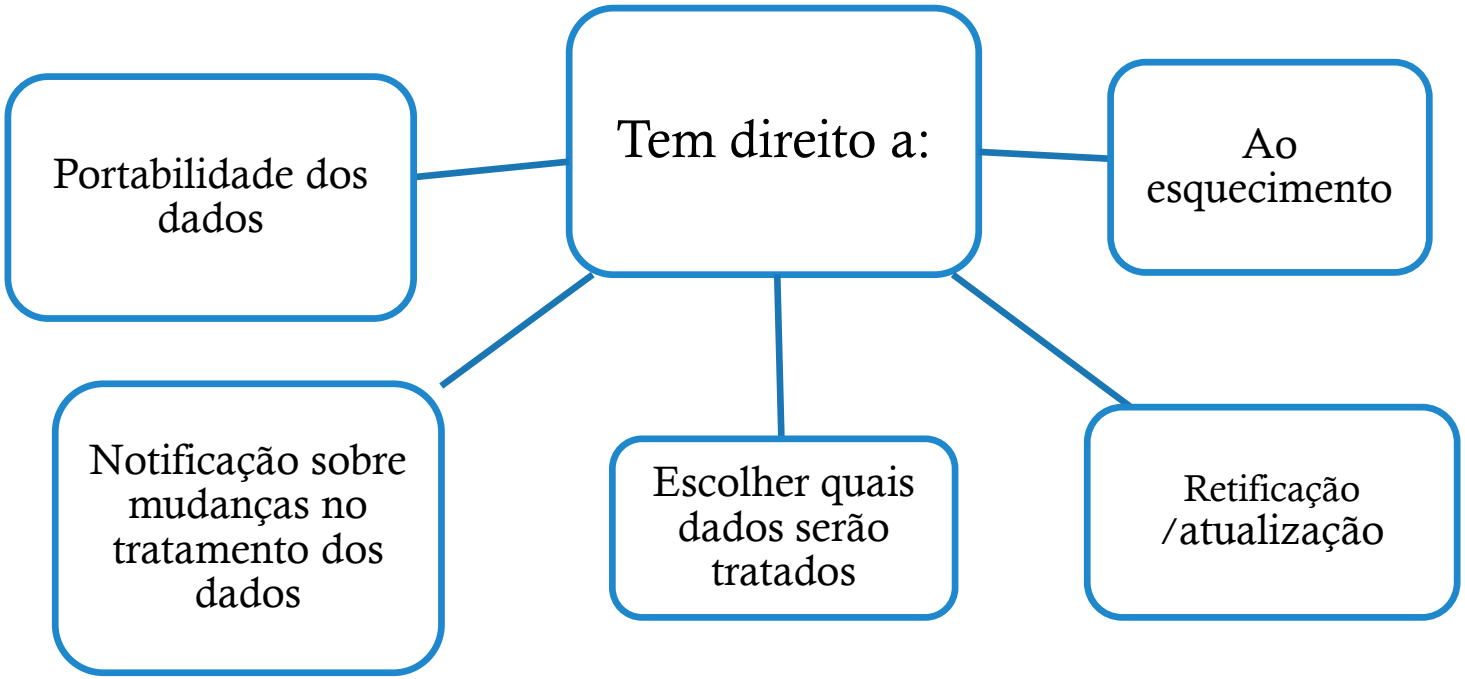
Não deve:

- Ser implícito
- “Check-box” já marcadas
- Agrupado com vários outros propósitos

GU Segurança

Direitos do Titular dos Dados

As regulamentações trazem mais **transparência** por parte das empresas e conferindo maior controle ao titular sobre seus dados.



GU Segurança

Notificação de Incidentes de Segurança

Notificações em caso de vazamento de **dados pessoais**:

GDPR

Notificar autoridade supervisora em até 72Hs

Comunicar o titular dos dados o mais breve possível

LGPD

Notifica futura autoridade supervisora, em prazo razoável

GU Segurança

Sanções

Multa de até 20 milhões de Euros ou até 4% do faturamento anual global, o que for maior.

GDPR

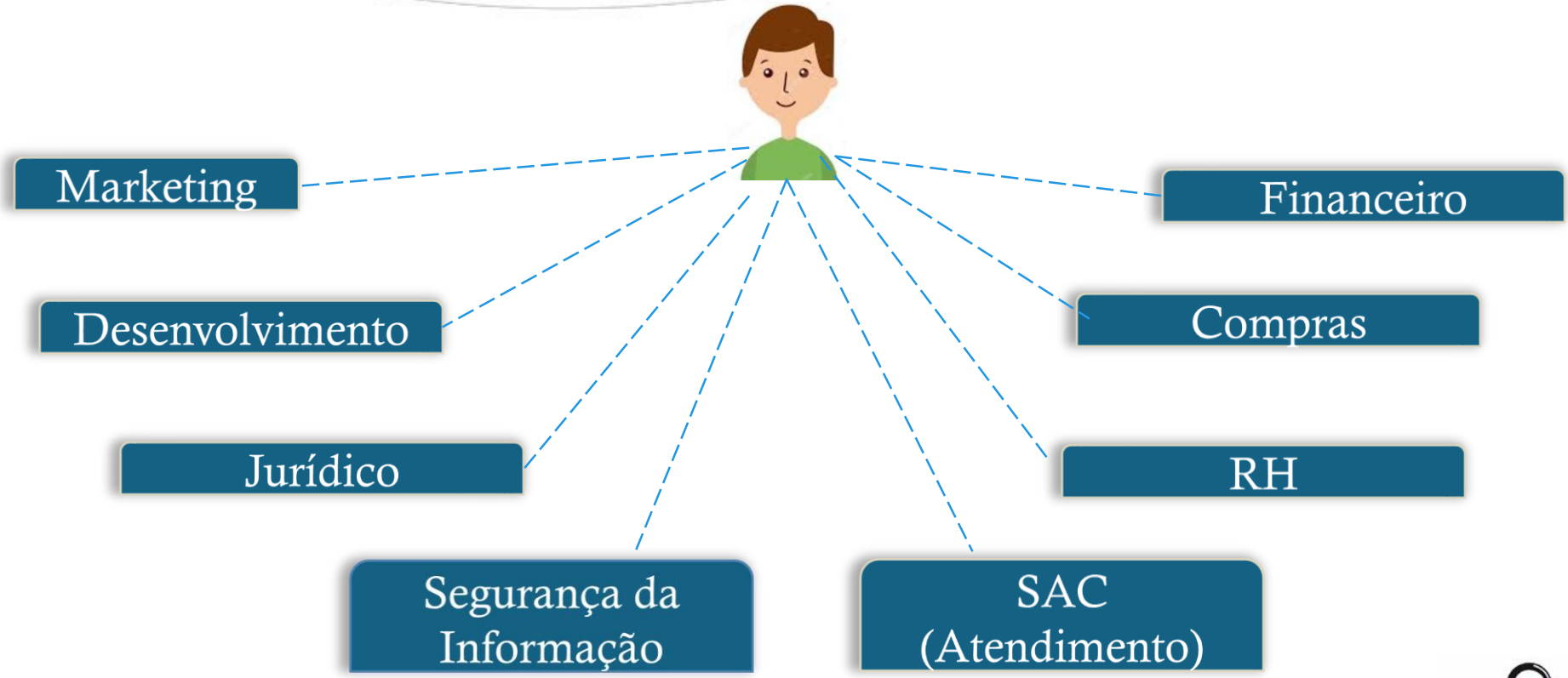
Advertência, multa de até 2% do faturamento, limitada a R$ 50 milhões por infração.

LGPD

Imagem → **Perda de clientes** → **Ecossistema ao redor**

GU Segurança

Principais áreas impactadas



GU Segurança

Responsável pela proteção de dados – DPO / APD

Data Protection Officer (DPO)

LGPD → Orienta a organização controladora a ter encarregado que responda pela proteção de dados pessoais.

GDPR → Orienta a organização a ter encarregado que responda pela proteção de dados pessoais.

Os dados do DPO deve constar na página da empresa, na política de privacidade. Ele deve ser o facilitador entre a organização e o órgão regulador.

GU Segurança

Conceito - Privacy by Design

Privacy by Design: aborda a proteção dos dados em todas as etapas do desenvolvimento do produto ou sistema.

Demora no tratamento dos dados equivale a maior custo na remediação. **(DPO pode ajudar)**

O que fazer para ficar compliance?

Contrate uma consultoria especializada em Direito Digital para:

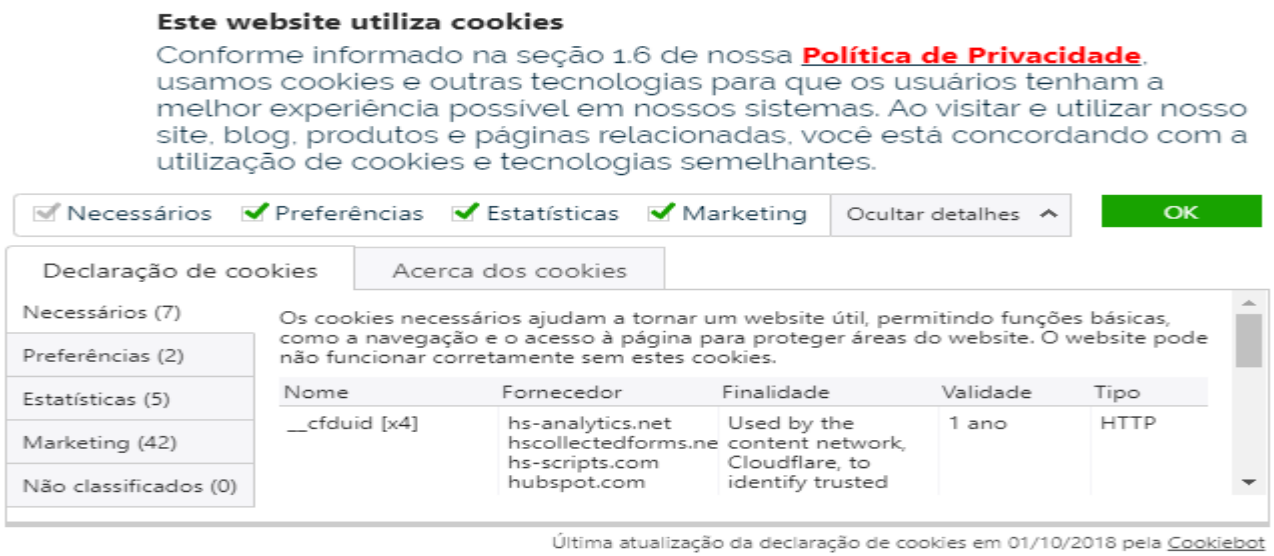
- ✓ Avaliação interna da organização
- ✓ Análise dos contratos atuais e confecção de novos modelos de contrato
- ✓ Assessoria jurídica

GU Segurança

O que fazer para ficar compliance?

- ✓ Ajustes de **coleta de cookies** nos sites e blogs da organização
- ✓ Atualização da **Política de Privacidade** para uso de cookies
- ✓ Solicitação de **consentimento** sempre que necessário **(Amigável)**

Exemplo:



GU Segurança

O que fazer para ficar compliance?

- ✓ Política de Segurança de Dados, com diretrizes sobre a manipulação, armazenamento e processamento de dados pessoais.

- ✓ Classificação dos dados sensíveis

- ✓ Mapeamento das bases de dados existentes:
  - Planilhas
  - Access
  - Ambientes de testes não oficiais

GU Segurança

O que fazer para ficar compliance?

- ✓ Implementação de um Data Loss Prevention (DLP)
- ✓ Assinatura de um termo de consentimento dos colaboradores da empresa sobre o uso dos seus dados pessoais para fins de empregabilidade
- ✓ Validação se seus fornecedores estão buscando adequação a regulamentação.

GU Segurança

O que fazer para ficar compliance?

- ✓ Auditoria para a manutenção dos requisitos implementados
- ✓ Criação de um comitê multi-disciplinar para apoiar as decisões do DPO
- ✓ Acordos de confidencialidade (NDA) para colaboradores e fornecedores
- ✓ Definição de um DPO

GU Segurança

O que fazer para ficar compliance?

- ✓ Treinamentos para conscientização dos colaboradores sobre mudança de cultura para manipulação de dados pessoais
- ✓ Criação de um comitê multi-disciplinar para apoiar as decisões do DPO
- ✓ xxxx
- ✓ xxxx

GU Segurança

Obrigado!

Paulo Oliveira

paulor1982@gmail.com
51 9 9997 7286

GU Segurança

SUCESU-RS
Associação dos Usuários de Informática e Telecomunicações do RS