GS1 Portugal

A Linguagem Global dos Negócios

NOVO REGULAMENTO DA PROTEÇÃO DE DADOS

Ação Informativa

4 de junho **14H00** Lisboa (Auditório GS1 Portugal)

Programa

14h00 – 14h30	**Credenciação**	
14h30 – 14h45	**Sessão de Abertura**	**João de Castro Guimarães** *Diretor Executivo* GS1 Portugal **Pedro Lima** *Consultor* GS1 Portugal **Mariana Bernardino Ferreira** *Advogada* BAPTISTA, MONTEVERDE & ASSOCIADOS
14h45 – 15h00	**RGPD e impactos na gestão dos Dados dos Colaboradores**	**Gregório Rocha Novo** *Advogado da CIP - Confederação da Industria Portuguesa*
15h00 – 15h30	**O que devemos saber sobre o RGPD e por onde começar?**	**Pedro Lima** *Consultor* GS1 Portugal
15h30 – 15h45	**4 Passos para implementar o RGPD na sua empresa**	
15h45 – 16h00	***Coffe-Break***	
16h00 – 16h45	**As questões mais comuns de Incumprimento** (inclui Perguntas & Respostas)	**Mariana Bernardino Ferreira** *Advogada* BAPTISTA, MONTEVERDE & ASSOCIADOS
16h45 – 17h00	**Encerramento** (inclui Perguntas & Respostas)	**Pedro Lima** *Consultor* GS1 Portugal
17h00 – 17h45	**(opcional) Visita ao Centro de Inovação e Competitividade**	

GS1 Portugal

A Linguagem Global dos Negócios

Regulamento Geral de Proteção de Dados (RGPD)

Contexto

Pedro Lima

04 de Junho de 2018

O que é o RGPD

O novo **Regulamento Geral de Proteção de Dados** da União Europeia entrou em vigor em **maio de 2018** e é a maior alteração às leis de privacidade em mais de vinte anos.

Vai obrigar a uma mudança significativa na forma como todas as empresas recolhem e tratam os dados pessoais, obrigando à implementação de **mecanismos de controlo** e de **capacidades de gestão** para garantir **a privacidade dos dados pessoais** que sejam recolhidos.

Aplicação e sanções

A aplicação da norma será acompanhada por um regulador e as empresas que não implementem medidas de compliance serão alvo de **coimas** que podem ir de **20 milhões de Euros** até **4% do volume de negócios** e sanções de natureza **civil** e **criminal**

"Atualmente, na Europa, só se verificam coimas ao mesmo nível na lei da concorrência."

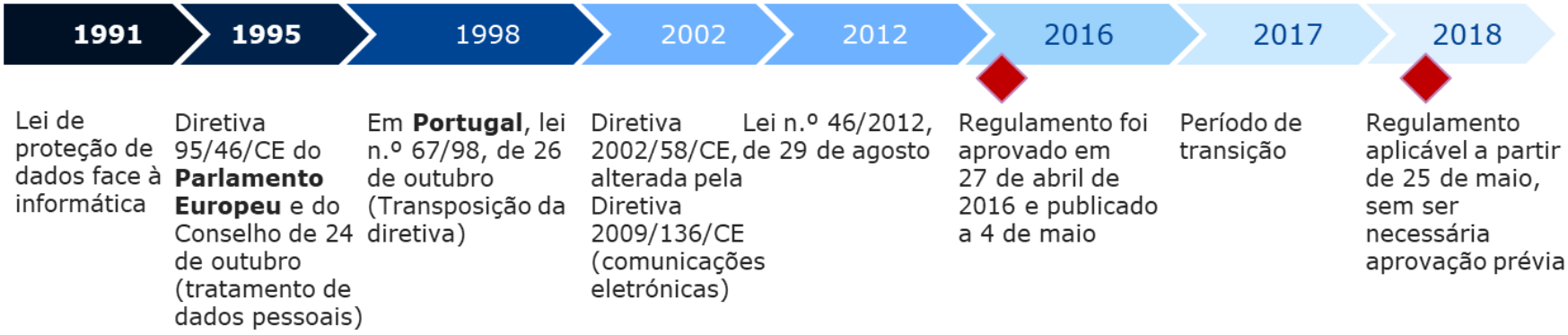
Âmbito

O RGPD respeita ao tratamento de **informações relativas a pessoas singulares** por uma organização.

Cobre todos os **dados suscetíveis de identificar um indivíduo**: nome, morada, NIF, etc, **mesmo que indiretamente:** IP de um PC de acesso, etc.

Abrange todas as operações envolvendo dados pessoais, tais como a recolha, registo, estruturação, conservação, alteração, recuperação, consulta, utilização, divulgação por transmissão, comparação ou interconexão, limitação, apagamento ou destruição.

O regulamento em contexto



Legislação em vigor há mais de 20 anos a nível nacional e europeu

GS1 Portugal

A Linguagem Global dos Negócios

Regulamento Geral de Proteção de Dados (RGPD)

Evento Informativo

Pedro Lima

4 de Junho de 2018

AGENDA

1. **Por onde começar**
2. Quatro Passos para implementar o RGPD (caso prático GS1)

Recordando: as mudanças mais relevantes são

- Mudança do paradigma de regulação externa, para **autorregulação**
- Deveres de **informação** e de obtenção de **consentimento explícito**
- Reforço dos **direitos dos titulares** dos dados (p.e. direito de eliminação)
- Dever de **notificação** em caso de violações de dados pessoais
- Obrigação de **conservação de um registo** das atividades de tratamento
- Imposição do tratamento dados numa lógica ***privacy by design*** e ***by default***
- Designação de encarregado da proteção de dados (**Data Protection Officer**)

Mas então o que é necessário fazer ?

Alguns exemplos de questões

- É possível não pedir autorização de recolha e tratamento de alguns dados pessoais ?
- Quais os dados que não posso pedir ou recolher ?
- Como tratar a lista dos nomes dos filhos dos funcionários para a festa de natal ?
- Ao criar uma folha excel a partir de outras fontes, estamos a criar uma nova base de dados ?
- Podemos mostrar a foto dos colaboradores na intranet ?
- Se tiver um serviço externo de contabilidade / jurídico / cobranças / tratamento de informação, como devo proceder ?
- Se houver transmissão de dados para o estrangeiro, como proceder ?

Sempre que haja dados pessoais, assumir que estão sujeitos ao RGPD

Todas as empresas tratam dados pessoais ?

Quando podem ser tratados os dados pessoais ?

Quando exista consentimento livre, informado, específico e expresso por parte dos respetivos titulares

Quando o tratamento seja essencial para a formação ou execução de um contrato (ex.: contrato de trabalho)

Quando exista um fundamento legal específico para o tratamento (ex.: comunicação de informação à AT)

Quando o tratamento seja efetuado para realizar um interesse legítimo do responsável pelo tratamento (ex. melhor qualidade de serviço)

Fonte: Soc. Advogados Morais Leitão (adaptado)

Avaliar grau de cumprimento do RGPD

Avaliar o grau de cumprimento do GDPR, analisando o tratamento dos dados pessoais dos três principais grupos de titulares

Avaliar cumprimento do RGPD

FUNCIONÁRIOS

CLIENTES

RESTANTES EXTERNOS

AGENDA

1. Por onde começar
2. **Quatro Passos para implementar o RGPD (caso prático GS1)**

Em Maio de 2017 colocámos a questão

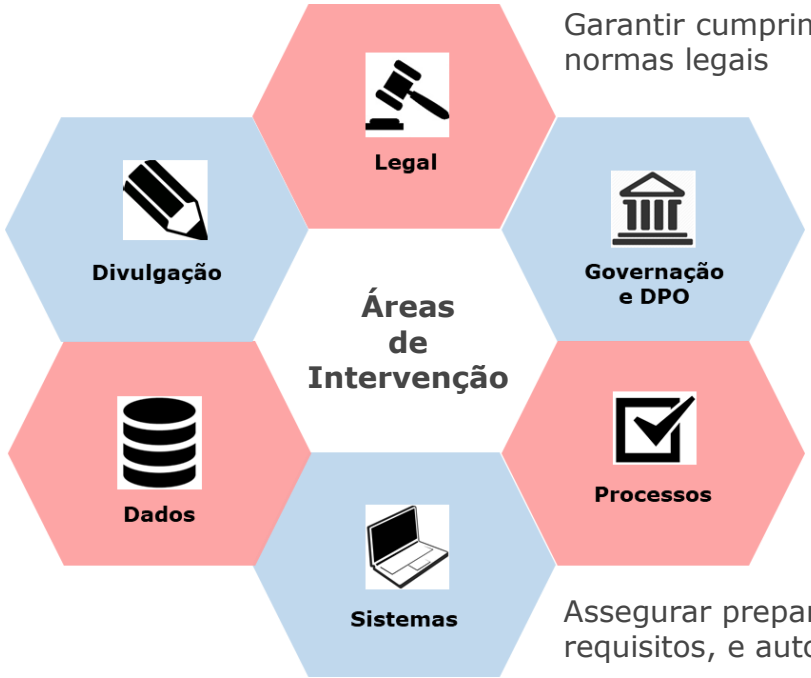
Tendo a GS1 um "negócio" B2B será que precisa mesmo de um projeto RGPD ?

Resposta : sim

Na GS1 o que pode estar em questão ?

- É preciso pedir autorização para recolha dos dados dos associados ?
- No caso de um ENI, os dados são pessoais ou da empresa ?
- E se alguém se recusar a fornecer os dados ?
- O que fazer aos dados dos associados que já temos em nossa posse ?
- Em que circunstâncias podemos contatar um associado ?
- Precisamos de pedir autorização para fazer uma campanha de marketing ?
- Podemos tratar os dados para efeitos estatísticos ?
- Podemos contatar os associados no caso de uma promoção ?
- Precisamos de um código de conduta ?

Adaptar a GS1 ao RGPD obrigou a atuar num vasto conjunto de áreas…



Garantir cumprimento das normas legais

Treinar as pessoas e garantir divulgação

Implementar a estrutura, nomear responsável pela proteção de dados e definir regras e atribuições

Inventariar e definir mecanismos de gestão

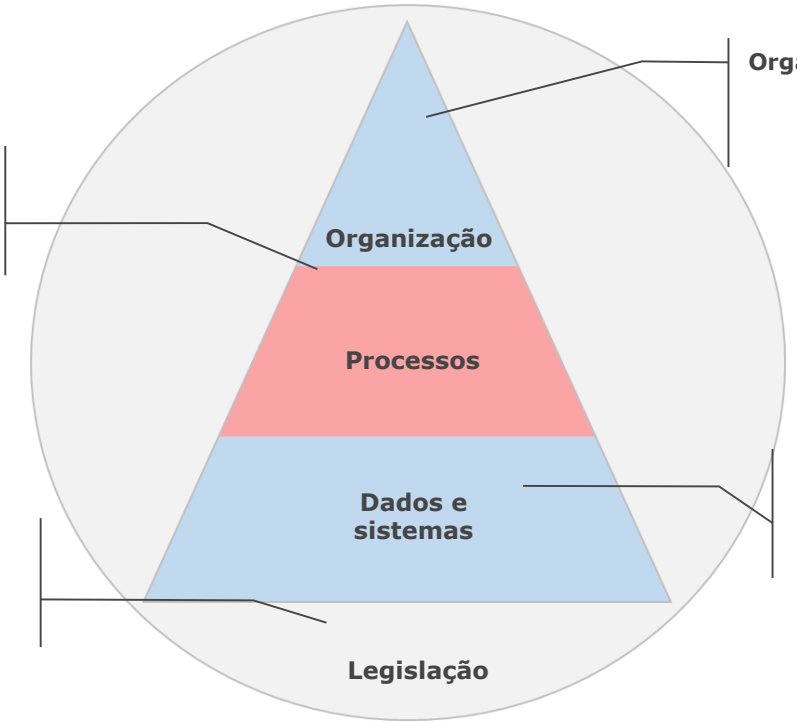
Implementar e monitorizar processos e procedimentos

Assegurar preparação e cumprimento dos requisitos, e automatizar o processo

O que implicou intervir nas dimensões de organização, processos, e dados e sistemas

Organização, Recursos Humanos e Governação
- Estruturar
- Formar e informar
- Responsabilizar

Processos e Procedimentos
- Rever
- Desenhar
- Implementar



Bases de Dados e Sistemas
- Confirmar Dados
- Adaptar Sistemas
- Automatizar Registos e Controlos

Cumprimento da RGPD
- Rever
- Adequar
- Elaborar

Concluímos que as adaptações necessárias obrigariam ao lançamento de um projeto

A dimensão das alterações impõe o desenvolvimento de um processo de adaptação interna de procedimentos, rotinas e regulamentação, e ainda um trabalho prévio de auditoria para identificação dos pontos críticos e necessidades específicas de adaptação.

Identificámos ser necessário atuar de imediato para garantir o cumprimento do RGPD até Maio de 2018

Decisão de avançar com projeto

Board da GS1 toma em Julho de 2017 a decisão de avançar com projeto

Definimos uma abordagem ao RGPD em quatro passos

A metodologia visa garantir e gerir a conformidade com o RGPD e inclui 4 fases, começando pela identificação da **finalidade** da recolha de informação

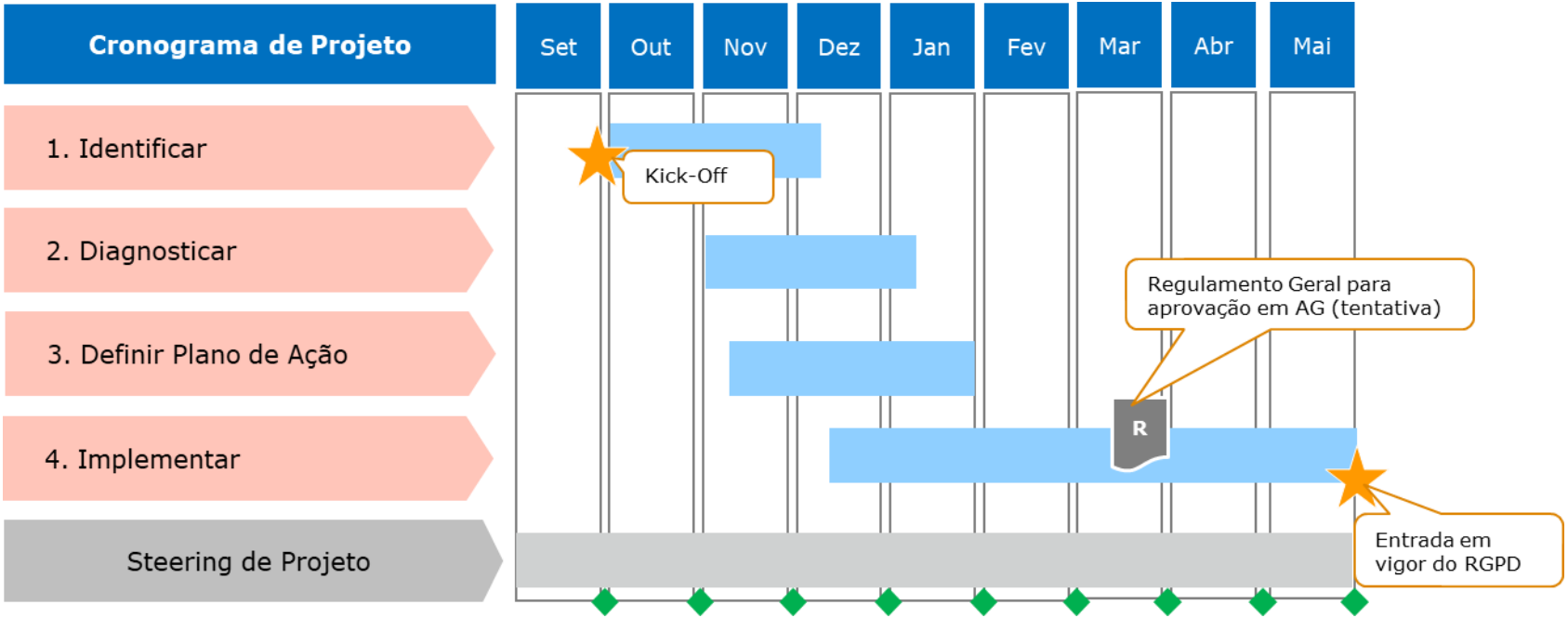
Identificar e caracterizar a finalidade para tratamentos de dados pessoais efectuados

Avaliar o nível de compliance com RGPD.

Implementar a iniciativas que assegurem a compliance com GDPR

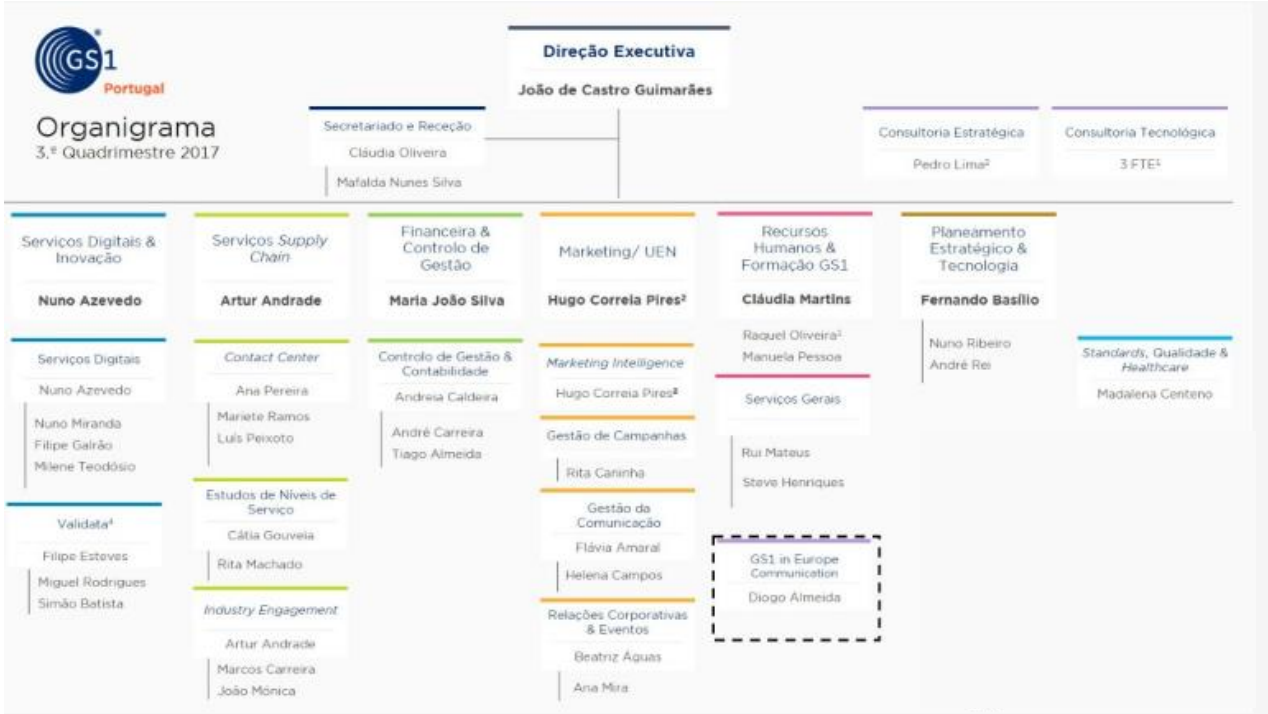
Definir ações em função do custo-benefício das alternativas e do grau de apetite ao risco

E um cronograma de projeto em 8 meses



Equipa de projeto – toda a organização

Equipa de projeto – toda a organização (cont.)



ETAPA 1 **Identificar**

Realizámos ações de preparação, divulgação e diversas reuniões com todas as áreas

- ✓ 2 apresentações pré-arranque aos diretores 1ª linha
- ✓ 1 apresentação pré-arranque aos 2ª linhas
- ✓ Sessão de preparação com o Advogado Tiago F. Costa (Morais Leitão)
- ✓ Kick-Off de Projeto
- ✓ Sessão de divulgação com toda a equipa GS1
- ✓ Reunião com CEO (Eng. João Guimarães)
- ✓ Entrevista com Assessora do CEO (Cláudia Oliveira)
- ✓ Entrevista com Comercial e Serviços Supply Chain (Artur Andrade+Ana Pereira+Mariete Ramos)
- ✓ Entrevista com Serviços Digitais e Inovação (Nuno Azevedo)
- ✓ Entrevista com Financeira e Controlo Gestão (M. João Silva+Andreia Caldeira+Tiago)
- ✓ Entrevista com Recursos Humanos e Formação (Cláudia Martins+R. Oliveira)
- ✓ Entrevista com Planeamento Estratégico e Tecnologia (Fernando Basílio)
- ✓ Entrevista com Marketing/UEN (Ana Mira+Rita Caninha)

ETAPA 2 Diagnosticar

Usamos listas de questões e formulários para diagnosticar toda a informação relevante.

1. Inventariação de todo o tipo de dados existentes para avaliar o ciclo de vida dos dados
2. Que dados ? de onde vêm? qual o formato? onde são guardados? para onde são transmitidos? quem tem acesso? de que forma acede? qual o propósito principal para o seu tratamento? qual o tempo de retenção?
3. Existem consentimentos?
4. Quais as tecnologias usadas para processamento, trasmissão, armazenamento, etc. papel, email, portal, servidores próprios, há teletrabalho? Dispositivos móveis
5. Quais os mecanismos e sistemas de proteção: antivírus, encriptação, firewalls/ VPNs, passowrds, backups

Registámos a informação em formulários próprios

Departamento de Recursos Humanos & Formação

Mapeamento de Dados Pessoais

Suporte	Dados Pessoais	Fonte de Licitude	Modo de Entrada dos Dados	Finalidade	Modo de Armazenamento	Responsável	Modo de Saída dos Dados	Propósito de Saída	Observações
Cópia do Cartão de Cidadão	Fotografia Nº de Utente de Saúde Nº Segurança Social Nº ID Civil Assinatura Nome de Ascendentes Data de Nascimento Nacionalidade Altura Sexo Data de Validade do CC		Enviado pela Entidade por e-mail ou em Pessoa	Celebração de Contrato de Trabalho	Cópia Guardada em Pasta no Computador do Funcionário Cópia Física Armazenada em Armário Trancado Documento Guardado no Outlook		N/A	N/A	
Ficha de Solicitação de Cartão	Fotografia Nome Função/Cargo		Enviado pelo Colaborador		Documentos Guardados no Outlook		Empresa Externa		

Confirmámos se em todos os casos podemos tratar dados pessoais.

Quando exista consentimento livre, informado, específico e expresso por parte dos respetivos titulares

Quando o tratamento seja essencial para a formação ou execução de um contrato (ex.: contrato de trabalho)

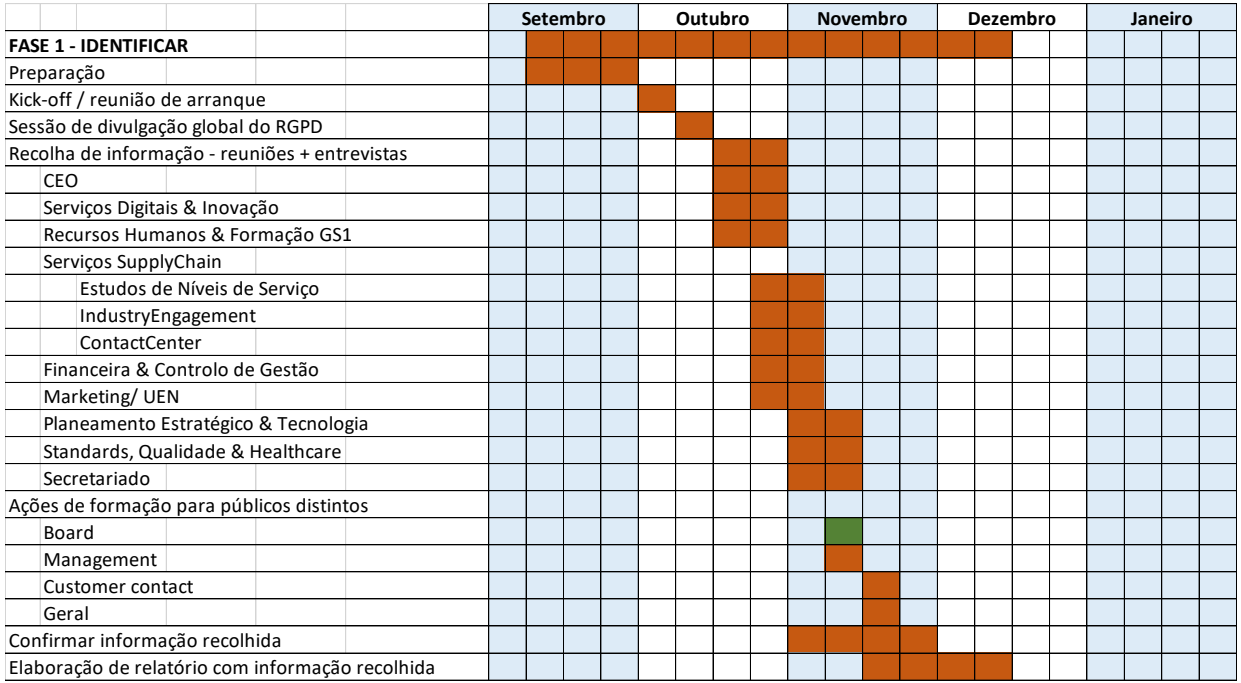
Quando exista um fundamento legal específico para o tratamento (ex.: comunicação de informação à AT)

Quando o tratamento seja efetuado para realizar um interesse legítimo do responsável pelo tratamento (ex. melhor qualidade de serviço)

Exemplos de questões identificadas no projeto

1. Sistema de acompanhamento de associados com moradas de alguns funcionários
2. Videovigilância (sem gravação de som)
3. Sistema de assiduidade com dados especiais
4. Armário com dossiers em papel, não protegido
5. Procedimento de agendamento de consultas externas num circuito em papel "visível"
6. Alguns computadores sem encriptação

ETAPA 3 Definir Plano de Ação



ETAPA 3 Definir Plano de Ação

		#	Tema	Responsável	Status	Prioridade	Deadline
		1	Regularizar Tratamento de Dados de Stakeholders	Cláudia Oliveira	Terminado	N/A	31/10/2017
23	Regular	2	Colocar Fechadura no Armário do Contact Center	Cláudia Martins	Terminado	N/A	25/05/2018
24	Regular	3	Eliminar Cópias de CC dos Associados nos Sistemas	Fernando Basílio	Terminado	N/A	25/05/2018
25	Regular	4	Eliminar Declarações de IRS nos Sistemas	Fernando Basílio	Terminado	N/A	25/05/2018
26	Implem	5	Eliminar Cópias Físicas dos CC dos Associados	Artur Andrade	Terminado	N/A	25/05/2018
27	Regular	6	Eliminar Cópias Físicas de Declarações de IRS	Artur Andrade	Terminado	N/A	25/05/2018
28	Regular	7	Garantir o Compliance do RGPD dos Fornecedores	1ª Linha	Terminado	N/A	25/05/2018
29	Regular	8	Elaborar uma Política de Privacidade Externa	Daniel Mattos	Terminado	N/A	01/03/2018
30	Regular	9	Elaborar uma Política de Privacidade Interna	Pedro Lima	Terminado	N/A	25/05/2018
31	Elabora	10	Elaborar um Manual de Procedimentos	Daniel Mattos	Em Realização [Final]	Alta	25/05/2018
32	Elimina	11	Validar o Conteúdo do Arquivo Físico Externo	Maria João Silva	Terminado	N/A	25/05/2018
33	Regular	12	Cumprir com as Regras de Videovigilância	Cláudia Martins	Terminado	N/A	25/05/2018
34	Regular	13	Cumprir com Regras de Verificação de Assiduidade	Cláudia Martins	Terminado	N/A	25/05/2018
35	Regular	14	Regularizar Procedimento do Seguro de Saúde	Cláudia Martins	Terminado	N/A	25/05/2018
36	Regular	15	Elaborar Formações de RGPD aos Departamentos	Pedro Lima	Aprovado	Média	25/05/2018
37	Regular	16	Reunir com o Diretor Executivo Acerca do RGPD	Pedro Lima	Terminado	N/A	25/05/2018
38	Regular	17	Reunir com Toda a 1º Linha Acerca do RGPD	Pedro Lima	Terminado	N/A	21/11/2017
39	Regular	18	Elaborar um Fluxograma Geral de Dados Pessoais	Daniel Mattos	Em Realização [Final]	Alta	25/05/2018
40	Elimina	19	Regularizar os Tratamento Futuros de Dados de ENI	Artur Andrade	Em Realização [Inicial]	Média	25/05/2018
41	Regular	20	Regularizar Tratamento dos Dados de ENI Associados	Artur Andrade	Em Realização [Inicial]	Alta	25/05/2018
42	Regular	21	Elaborar de Mensagem de Voz para Contact Center	Artur Andrade	Terminado	N/A	25/05/2018
43	Regular	22	Elaborar de Mensagem Escrita para o Chat	Artur Andrade	Terminado	N/A	25/05/2018
44	Regularizar Campanhas de Marketing			Hugo Pires	Terminado	N/A	25/05/2018

ETAPA 4 Implementar as iniciativas

1. Mobilização de toda a estrutura
2. Atuação continuada e com base em quick-wins
3. Elaboração de Política de privacidade
4. Procedimentos para sistemas de informação
5. Contato informativo com associados
6. Elaboração de clausulado contratual com fornecedores
7. Elaboração de acordo com colaboradores
8. Formação das pessoas chave
9. Implementação de todas as iniciativas

Questões

Dra. Mariana Ferreira
BAPTISTA, MONTEVERDE & ASSOCIADOS Sociedade de Advogados

As questões mais comuns de Incumprimento