PRIVACY & DATA PROTECTION PRACTITIONER

Bem-vindo!!! Welcome! Bienvenido!

- Muito obrigado por escolher um treinamento oficial do *HSI Institute*!
- Temos o prazer de tê-los como alunos e de transmitir toda a nossa experiência e conhecimento de maneira única e inovadora aos nossos clientes.

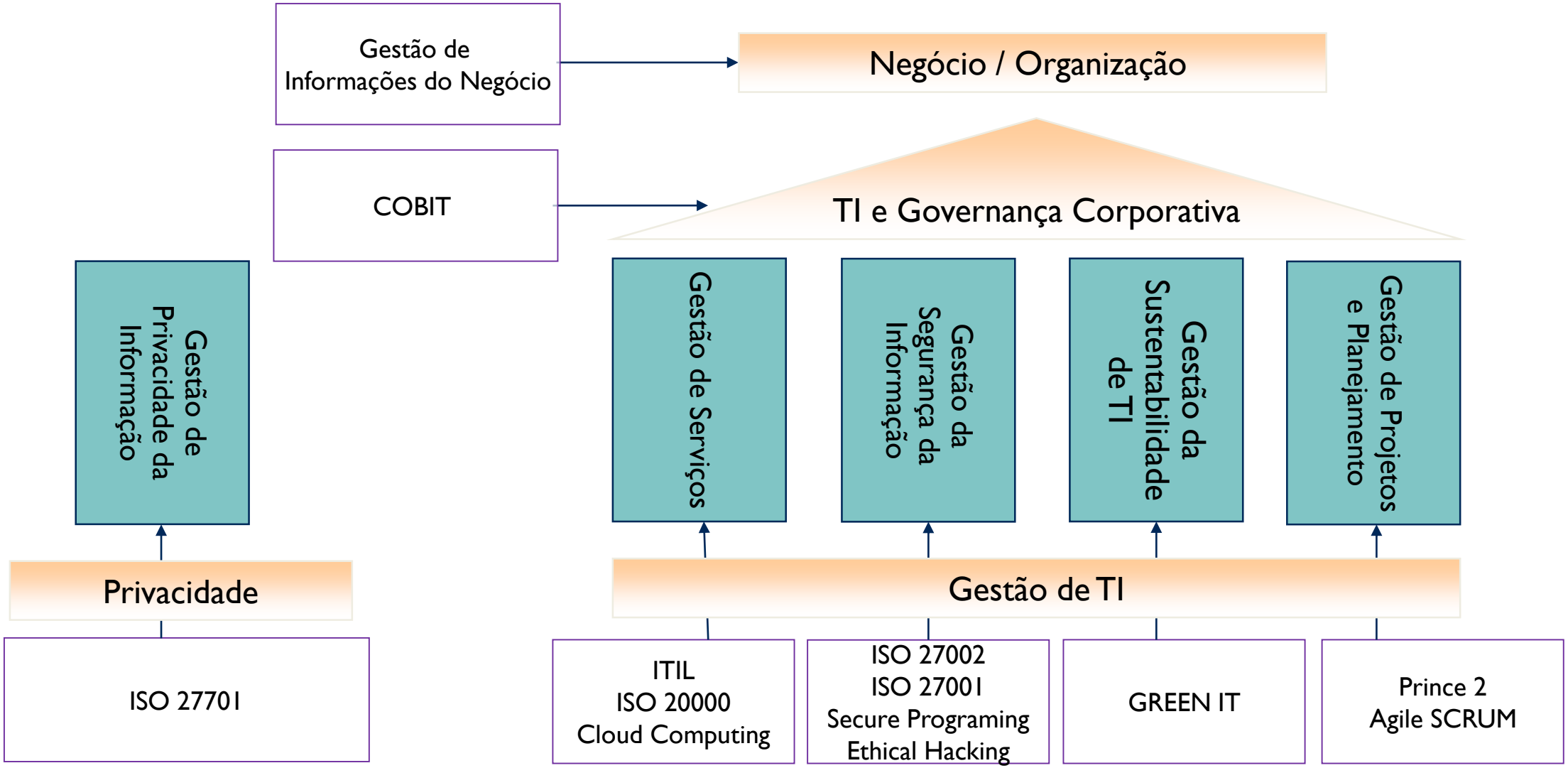
HSI Institute

O maior instituto em conteúdo voltado a treinamentos em Governança de TI.

HSI é um parceiro oficial credenciado pelos maiores centros certificadores da área: EXIN e PeopleCert.

Provedor de Conteúdo Oficial para a rede de provedores de treinamentos credenciados.

Fique conectado com outros treinamentos e conteúdos oficiais HSI



Versão 1.3 – 12/2020.

Check-In

Breve apresentação

Experiência profissional

Objetivo

DATA PROTECTION OFFICER

PRIVACIDADE

CONSENTIMENTO

GDPR

ÂMBITO

NOTIFICAÇÃO

DIREITO DAS PESSOAS FÍSICAS

PORTABILIDADE

DIREITO DIGITAL

DPO/
CONTROLADOR/
PROCESSADOR

DPIA

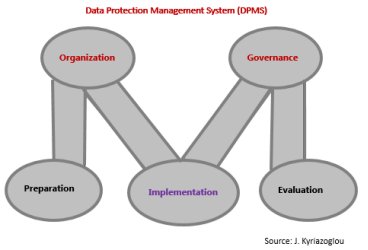
PD&P
BY DESIGN

GDPR PRACTITIONER

PD&P
BY DEFAULT

VIOLAÇÃO/
NOTIFICAÇÃO/
RESP. A
INCIDENTES

SGPD



POLÍTICA DE
PRIVACIDADE

POLÍTICA DE
PROTEÇÃO DE
DADOS PESSOAIS

Agenda

Dia 1

0 - Introdução
1 - Políticas de proteção de dados pessoais e privacidade.
2 - Gerenciando e organizando a proteção de dados pessoais (Parte 1).

Dia 2

2 - Gerenciando e organizando a proteção de dados pessoais (Parte 2).
3 - Papéis e Responsabilidades: Controlador, Processador e *Data Protection Officer*.
4 - Avaliação de Impacto sobre a Proteção de Dados (DPIA, em inglês).

Dia 3

5 - Violação de dados pessoais, Notificação e Resposta a Incidentes.
6 - Atividades Práticas.
7 - Encerramento.

Agenda

Dia 1

0. Introdução
1. Políticas de proteção de dados pessoais e privacidade:
   - 1.1 Entendimento das necessidades de Políticas, Normas e Procedimentos;
   - 1.2 Conteúdo das Políticas, Normas e Procedimentos;
   - 1.3 Proteção de dados pessoais *by design* e *by default*:
     - 1.3.1 Princípios da proteção de dados pessoais *by design* e *by default;*
     - 1.3.2 Descrever os 7 princípios de proteção *by design* e *by default* e
     - 1.3.3 Implementação dos princípios de proteção de dados pessoais *by design* e *by default.*
2. Gerenciando e organizando a proteção de dados pessoais:
   Sistema de Gestão de Proteção de Dados Pessoais:
   - 2.1 Preparação;
   - 2.2 Organização;
   - 2.3 Desenvolvimento e Implementação;
   - 2.4 Governança e
   - 2.5 Avaliação e Melhoria Contínua.

Agenda

Dia 2

3. Papéis e Responsabilidades do Controlador, Processador e DPO:
   - 3.1 Papéis e Responsabilidades do Controlador e do Processador:
     - 3.1.1 Responsabilidades do Controlador;
     - 3.1.2 Responsabilidades do Processador e
     - 3.1.3 Relacionamento entre Controlador e Processador.
   - 3.2 Papéis e Responsabilidades do DPO:
     - 3.2.1 Quando é mandatória a indicação do DPO;
     - 3.2.2 Papel e responsabilidade do DPO e
     - 3.2.3 Relação do DPO com a Autoridade Supervisora.

4. Avaliação de Impacto sobre a Proteção de Dados (DPIA):
   - 4.1 Critérios para a condução de uma DPIA:
     - 4.1.1 Aplicação dos critérios para condução de uma DPIA e
     - 4.1.2 Descrever os objetivos e entregáveis de uma DPIA.
   - 4.2 Etapas de uma DPIA:
     - 4.2.1 Descrever as etapas de uma DPIA e
     - 4.2.2 Realizar uma DPIA em uma situação específica.

Agenda

Dia 3

5. Violação de dados pessoais, Notificação e Resposta a Incidentes:
   - 5.1 Requisitos do GDPR em relação à violação de dados pessoais:
     - 5.1.1 Avaliar se ocorreu uma violação de dados pessoais de acordo com o GDPR.
   - 5.2 Requisitos para notificação:
     - 5.2.1 Quando notificar a Autoridade Supervisora;
     - 5.2.2 Quando notificar o Titular dos Dados Pessoais e
     - 5.2.3 Elementos obrigatórios em uma notificação.

6. Atividades Práticas:
   - 6.1 Papéis e Responsabilidades: Controlador, Processador e DPO;
   - 6.2 DPIA e
   - 6.3 Violação de Dados Pessoais: Plano de Resposta.

7. Encerramento.

Público Alvo e Pré-Requisitos

Esta certificação de nível profissional será particularmente útil para:

- DPO- Data Protection Officer/Ponto Focal;
- Jurídico;
- Compliance;
- CISO – Chief Information Security Officer;
- Gerente de Continuidade de Negócios;
- Auditor de proteção de dados pessoais (interno e externo) e
- Recursos Humanos.

Pré-requisitos:

Nenhum.

No entanto, como essa certificação está em um nível avançado, as certificações <u>prévias</u> do EXIN ISFS e P&DPF são altamente recomendadas.

Objetivos do Curso

Proporcionar o entendimento sobre:

- Políticas de privacidade e proteção de dados pessoais;
- Proteção de dados pessoais *by design e by default*;
- Papéis e responsabilidades do Controlador, Processador e DPO;
- DPIA - Avaliação de Impacto sobre a Proteção de Dados e
- Violação de Dados Pessoais, Notificação e Resposta a Incidentes.

Ter a capacidade de elaborar/aplicar/realizar/explicar/justificar:

- A existência das políticas, normas e procedimentos;
- 7 princípios da proteção de dados pessoais *by design e by default;*
- As fases do Sistema de Gestão de Proteção de Dados;
- O programa de conscientização sobre proteção de dados pessoais;
- Papéis e responsabilidades do Controlador, Processador e DPO;
- Os critérios para uma avaliação de impacto sobre a proteção de dados (DPIA);
- As etapas de uma avaliação de impacto sobre a proteção de dados (DPIA);
- Os requisitos do GDPR sobre às violações de dados pessoais e
- Os requisitos para notificação quando da violação de dados pessoais.

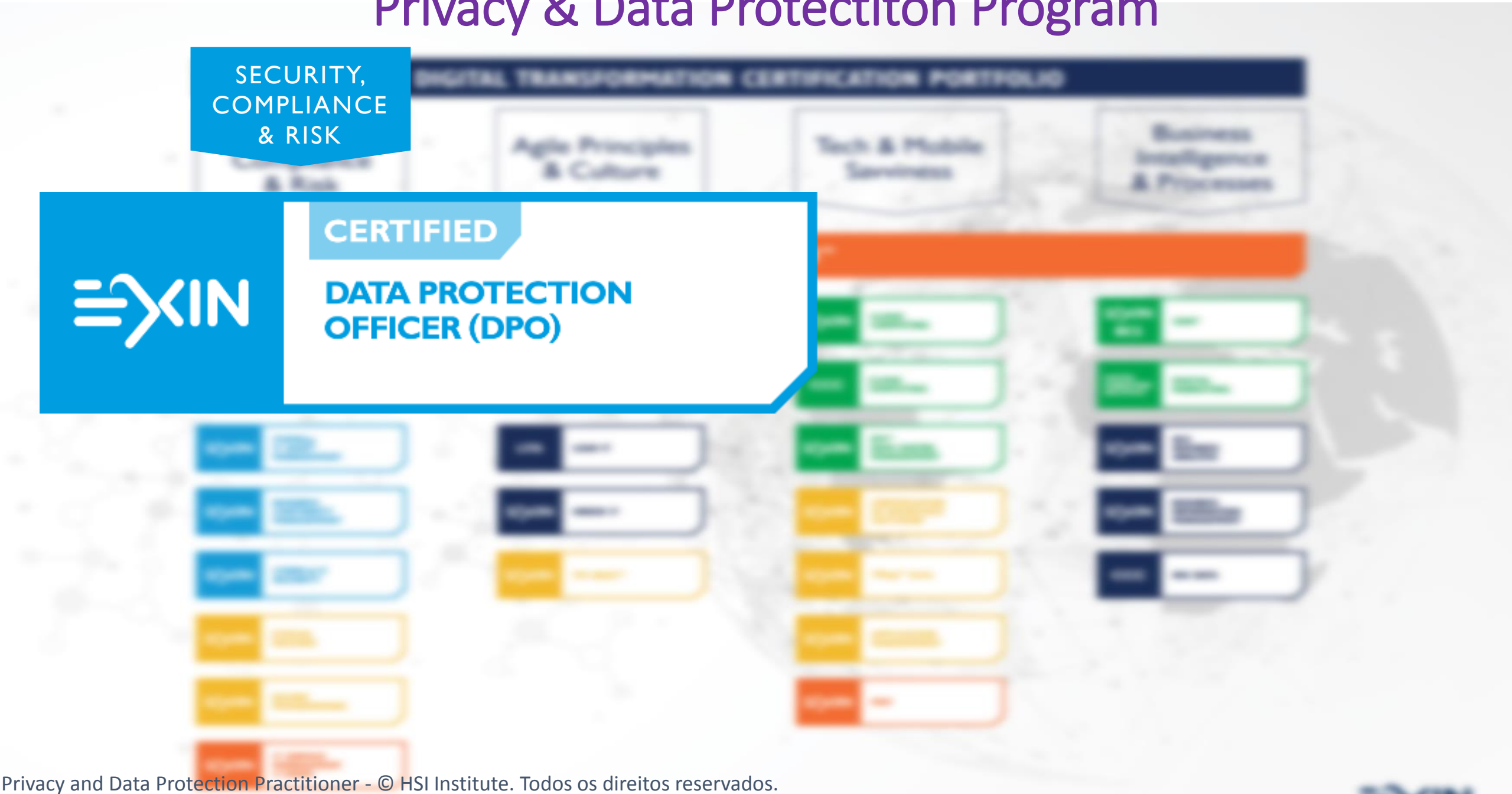
Privacy & Data Protectiton Program

SECURITY, COMPLIANCE & RISK

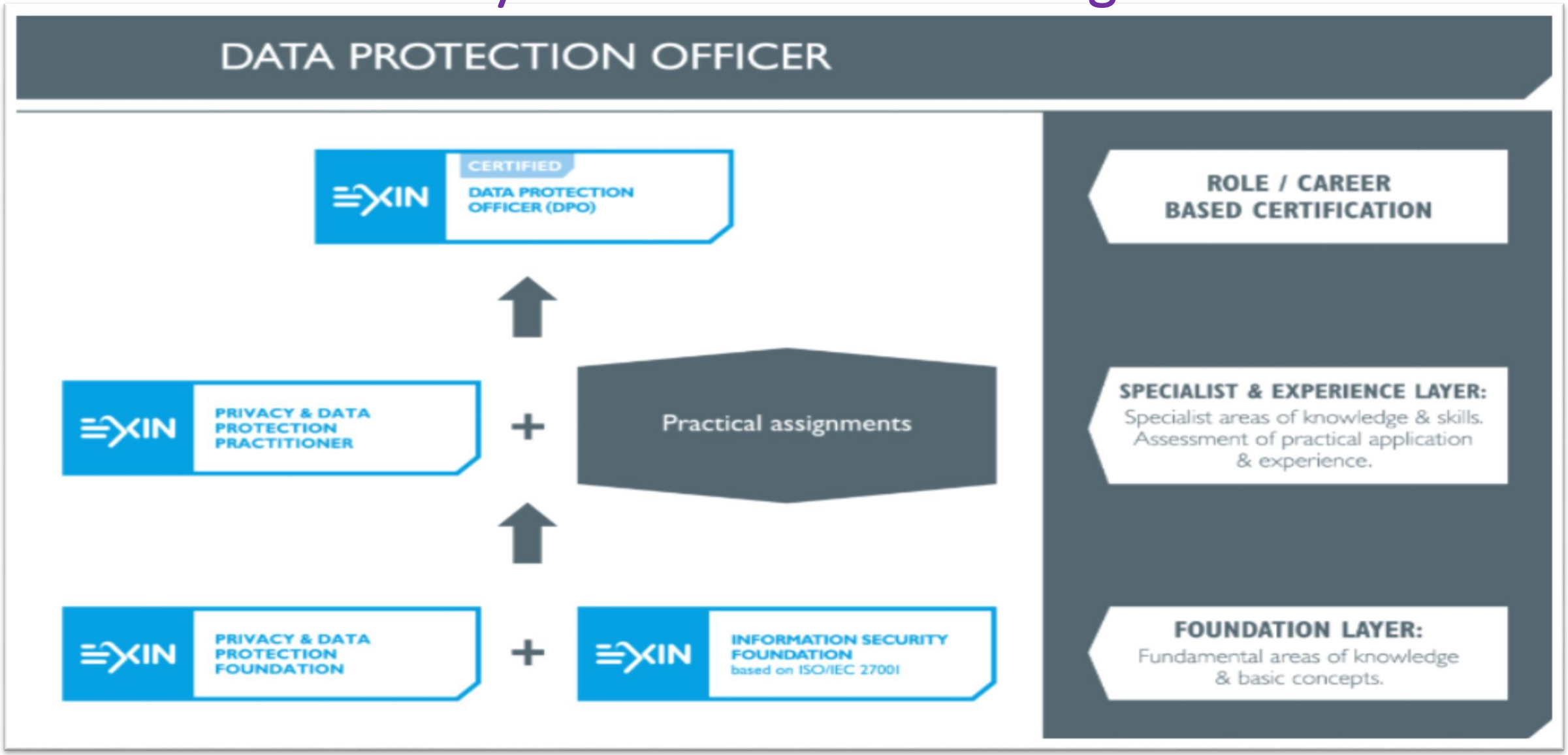
EXIN

CERTIFIED

DATA PROTECTION OFFICER (DPO)



Privacy & Data Protectiton Program



FORMAÇÃO DPO – DATA PROTECTION OFFICER
ROLE BASED CERTIFICATION

ISF

+

PDPF

+

PDPP

=

FOUNDATION LAYER:
Fundamental areas of knowledge & basic concepts

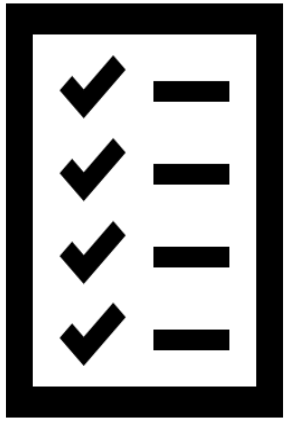
SPECIALIST & EXPERIENCE LAYER:
Specialist areas of knowledge & skills, Assessment of practical application & experience

Todas as provas em português

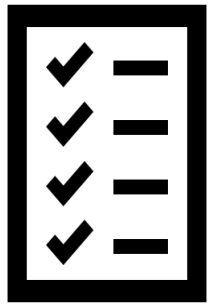
Requisitos para Certificação PDP&P

Conclusão bem sucedida do exame EXIN Privacy & Data Protection Practitioner.

Curso de P&DPP junto a credenciado EXIN, incluindo a conclusão das atividades práticas.



Formato do Exame PDP&P Practitioner



Tipo de exame: questões de múltipla escolha.

Número de questões: 40.

% mínimo para aprovação: 65%.

Com consulta: O texto do GDPR pode ser consultado durante todo o exame.

Vedado acesso a equipamentos eletrônicos.

Tempo máximo: 120 minutos.

As regras e regulamentos das provas do EXIN serão aplicadas para este exame de certificação.

Peso de Cada Tema do Exame

Requisito do exame	Especificação do exame	Peso
1. Políticas de proteção de dados		**10%**
	1.1 O objetivo das políticas de proteção de dados e privacidade em uma organização	5%
	1.2 Proteção de dados desde a concepção (by design) e por padrão (by default)	5%
2. Gerenciando e organizando a proteção de dados		**32,5%**
	2.1 Fases do Sistema de Gestão de Proteção de Dados (SGPD).	32,5%
3. Papéis do controlador, processador e Data Protection Officer (DPO)		**17,5%**
	3.1 Os papéis do controlador e processador	10%
	3.2 O papel e as responsabilidades de um DPO	7,5%
4. Avaliação de Impacto sobre a Proteção de Dados (DPIA)		**27,5%**
	4.1 Os critérios para uma DPIA	15%
	4.2 As etapas de uma DPIA	12,5%
5. Violação de dados, notificação e resposta a incidentes		12,5%
	5.1 Os requisitos do GDPR em relação a violações de dados pessoais	2,5%
	5.2 Os requisitos para notificação	10%
	Total	**100%**

Contexto

O GDPR e outras literaturas "informam **por que** você precisa de proteção para os dados pessoais".

Políticas "dizem **o que** fazer para à proteção de dados pessoais".

Planos, Procedimentos, P**ráticas** e C**ontroles** "informam **como** fazer isso".

As pessoas e outros recursos (budget, tecnologia, etc.) definem "**quais** recursos devem ser utilizados para atingir o nível adequado de proteção de dados pessoais".

Contexto

As **políticas** são detalhadas na especificação de requisitos do exame 1.1.

- Como políticas, planos, etc. e as pessoas interagem e trabalham juntas para proteção de dados pessoais são apresentadas nas especificações dos requisitos do exame **2 (SGPD)** e **3 (Controlador**, etc.).
- Como o GDPR afeta a empresa, seus produtos e serviços e os titulares de dados, as medidas a serem implementadas para proteção dos dados pessoais estão detalhadas nas especificações dos requisitos do exame **1.2.** (**Proteção de dados pessoais *by design e by default***), **4 (DPIA)** e **5 (Violação de dados pessoais).**

Conceitos Básicos

Presumem-se já conhecidos pelo aluno os conceitos básicos *Privacy & Data Protection Pratictioner (**P&DPP**)* e *Privacy & Data Protection Foundation (**P&DPF**)*.

A pesquisa e a compreensão dos referidos conceitos são requisitos necessários para realização do exame.

Os conceitos básicos de ***P&DPP*** e de ***P&DPF*** podem ser encontrados nos respectivos guias de preparação.

Valor da Certificação PDP&P

- Importância crescente da proteção da privacidade das pessoas e de seus dados;
- Entendimento das questões éticas, profissionais e de marketing digital no manuseio de dados pessoais;
- Surgimento de novas leis, por exemplo: *California Consumer Privacy Act* (2018) e LGPDP (Brasil), que foram criadas para regular o assunto privacidade e proteção de dados pessoais;
- Obrigatoriedade de cumprimento da legislação por parte de todas organizações envolvidas e
- Foco no desenvolvimento e implementação de políticas e procedimentos a fim de cumprir as legislações existentes e se adequar às futuras; com o estabelecimento de um sistema de gestão de proteção de dados pessoais para aplicação eficaz das diretrizes e melhores práticas de proteção de dados pessoais e privacidade.

Programação de Estudo

Literatura para o exame

A) IT Governance Privacy Team
EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide.
IT Governance Publishing, Cambridgeshire (second edition, 2017).
ISBN 978-1-84928-9450 (versão impressa).
ISBN 978-1-84928-9474 (e-book).

B) Kyriazoglou, J.
Data Protection and Privacy Management System. Data Protection and Privacy Guide - Vol. 1.
bookboon.com (first edition, 2016).
ISBN 978-87-403-1540-0.

Literatura Adicional

C. Comissão Europeia
Regulamento Geral de Proteção de Dados (GDPR) (Regulamento (UE) 2016/679)
Regulamento do Parlamento Europeu e do Conselho da União Europeia. Bruxelas, 27 de abril de 2016, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

D. Grupo de Trabalho do Artigo 29.º Para a Proteção de Dados
Orientações sobre os encarregados da proteção de dados (EPD), wp 243rev.01, 5 de abril de 2017, disponível em http://ec.europa.eu/newsroom/Artigo29/item-detail.cfm?item_id=612048

E. Grupo de Trabalho do Artigo 29.º Para a Proteção de Dados
Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, wp248rev.01, 4 de abril de 2017, disponível em http://ec.europa.eu/newsroom/Artigo29/item-detail.cfm?item_id=611236

F. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

G. ISO/IEC 27701:2019 (EN)
Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines
Suíça, ISO/IEC, 2019
https://www.iso.org/home.html

Literatura Adicional

Com relação à literatura C:

- Regulamentos, Diretrizes e outros atos. Os objetivos estabelecidos nos tratados da UE são alcançados por meio de vários tipos de atos jurídicos. Alguns são vinculativos e outros não. Alguns se aplicam a todos os países da UE, outros a apenas alguns. Um "regulamento" é um ato legislativo vinculativo. Deve ser aplicado na sua totalidade em toda a UE.
- Fonte de referência: https://europa.eu/european-union/law/legal-acts_en.
- O uso dos verbos (modais) “deve” e “deveria estar” no GDPR:
  - “Deve” expressa uma "lei ou regra“. É mandatório que você siga essa lei ou regra.
  - “Deveria estar” expressa uma expectativa. É recomendado que você siga esse conselho.
  - Nos padrões ISO, ele é usado de maneira semelhante: https://www.iso.org/foreword-supplementary-information.html:
    - “shall” indicates a requirement;
    - “should” indicates a recommendation;
    - “may” indicates a permission and;
    - “can” indicates a possibility or a capability.

Continua…

Literatura Adicional

Continuação...

Com relação às literaturas D & E:

- O Grupo de Trabalho de Proteção de Dados do Artigo 29* é composto por:
  - um representante da(s) autoridade(s) de supervisão designada(s) de cada país da UE;
  - um representante da(s) autoridade(s) estabelecida(s) para as instituições e organismos da EU e
  - um representante da Comissão Europeia.

*Desde de 25 de maio de 2018, o Grupo de Trabalho do Artigo 29 deixou de existir e foi substituído pelo *European Data Protection Board (EDPB*) e é composto pelas autoridades supervisoras de cada Estado-Membro e pelo *European Data Protection Supervisor (EDPS.*)

O site do *EDPB* pode ser consultado nos seguintes endereços:
https://edpb.europa.eu/edpb_en
https://edpb.europa.eu/edpb_pt

Bibliografia Online

European Commission

- General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 2016, available at http://eur-lex.europa.eu.

PDF:
http://eur-lex.europa.eu/legal-content/**EN**/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=**EN/PT**

HTML:
http://eur-lex.europa.eu/legal-content/**EN**/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=**EN/PT**

Bibliografia Adicional*

- ABNT NBR ISO/IEC 29100 - ESTRUTURA DE PRIVACIDADE
- ABNT NBR ISO/IEC 29134 - AVALIAÇÃO DE IMPACTO DA PRIVACIDADE
- ABNT NBR ISO/IEC 29151 - CÓDIGO DE PRÁTICA PARA PROTEÇÃO DE DADOS PESSOAIS
- ABNT NBR ISO/IEC 27001 - SGSI
- ABNT NBR ISO/IEC 27002 - CONTROLES SGSI
- ABNT NBR ISO/IEC 27003 - DIRETRIZES PARA IMPLANTAÇÃO DE UM SGSI (PUBLICADA 24/04/2020)
- ABNT NBR ISO/IEC 27005 - GESTÃO DE RISCOS EM SI.
- ABNT NBR ISO/IEC 27018 - PROTEÇÃO DE DP EM NUVENS PÚBLICAS QUE ATUAM COMO OPERADORES DE DADOS PESSOAIS
- ISO/IEC 27035 - GESTÃO DE INCIDENTES DE SI PARTE 3: DIRETRIZES PARA OPERAÇÕES DE RESPOSTAS A INCIDENTES DE TIC, ALINHADA E ORIENTADA PARA À GESTÃO DA PRIVACIDADE DA INFORMAÇÃO
- ABNT NBR ISO/IEC 27701 - EXTENSÃO DAS ABNT NBR ISO/IEC 27001 E 27002 PARA GESTÃO DA PRIVACIDADE DA INFORMAÇÃO

*** A Bibliografia Adicional destina-se exclusivamente à referência e aprofundamento do conhecimento**

Tabela ISO 27701 e GDPR

Subseção deste documento	Artigos do GDPR
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7),(42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.2.2	(5)(1)(f)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.2	(5)(1)(f)

Tabela ISO 27701 e GDPR

Tabela D.1 (continuação)

Subseção deste documento	Artigos do GDPR
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(f)
6.8.2.9	(5)(1)(f)
6.9.3.1	(5)(1)(f), (32)(1)(c)
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)
6.10.2.4	(5)(1)(f), (28)(3)(b), (38)(5)

Tabela ISO 27701 e GDPR

6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.1	(25)(1)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)
6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)

Tabela ISO 27701 e GDPR

Tabela D.1 (continuação)

Subseção deste documento	Artigos do GDPR
7.2.3	(8)(1), (8)(2)
7.2.4	(7)(1), (7)(2), (9)(2)(a)
7.2.5	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
7.2.6	(5)(2), (28)(3)(e), (28)(9)
7.2.7	(26)(1), (26)(2), (26)(3)
7.2.8	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)

Tabela ISO 27701 e GDPR

6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.1	(25)(1)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)
6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)

Tabela ISO 27701 e GDPR

7.3.3	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
7.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
7.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
7.3.6	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
7.3.7	(19)
7.3.8	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
7.3.9	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
7.3.10	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
7.4.1	(5)(1)(b), (5)(1)(c)
7.4.2	(25)(2)
7.4.3	(5)(1)(d)
7.4.4	(5)(1)(c), (5)(1)(e)
7.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
7.4.6	(5)(1)(c)
7.4.7	(13)(2)(a), (14)(2)(a)

Tabela ISO 27701 e GDPR

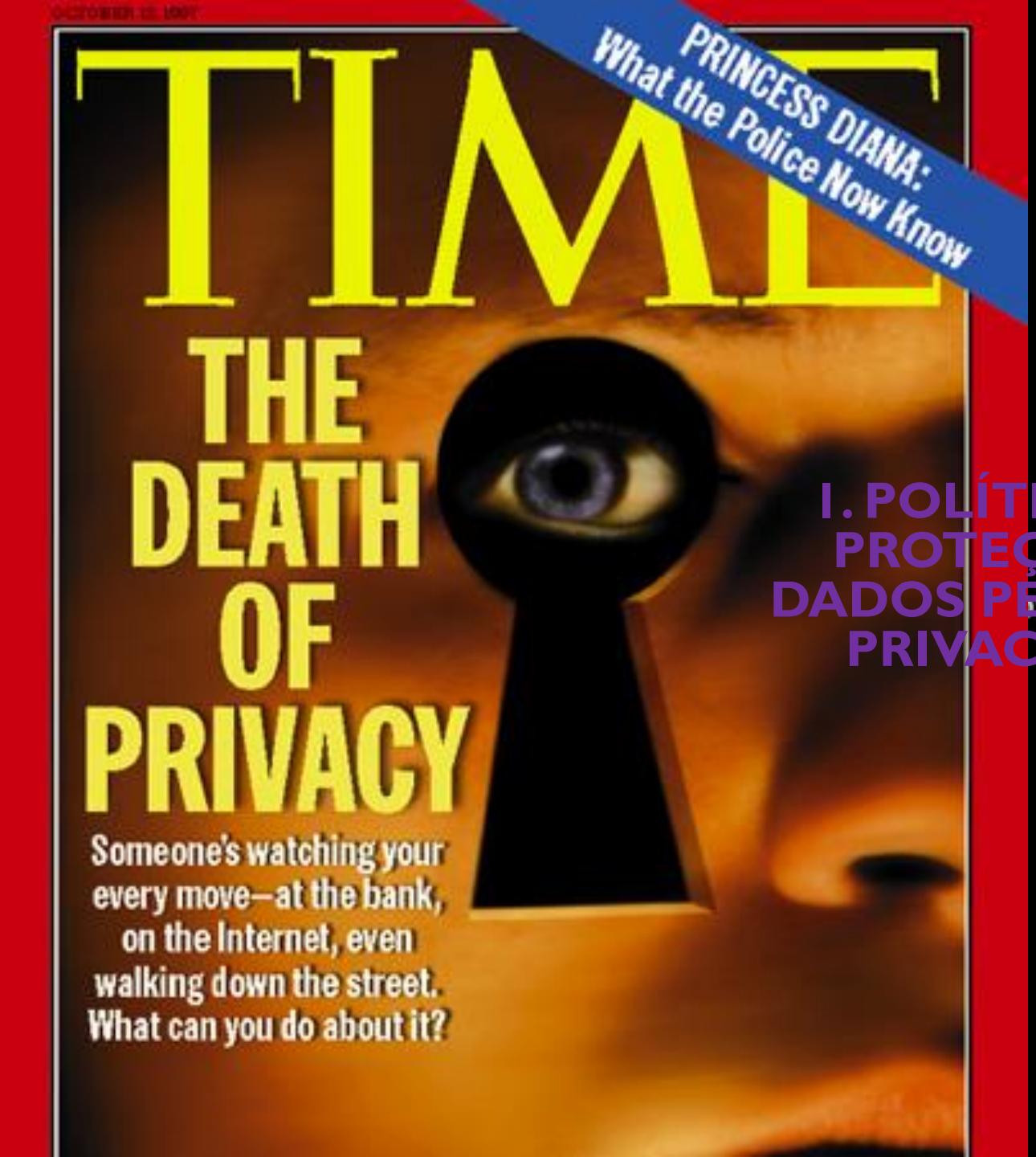
Subseção deste documento	Artigos do GDPR
7.4.8	(5)(1)(f)
7.4.9	(5)(1)(f)
7.5.1	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
7.5.2	(15)(2), (30)(1)(e)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
8.2.1	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)
8.2.2	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(h)
8.2.5	(28)(3)(h)

Tabela ISO 27701 e GDPR

8.2.6	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
8.3.1	(15)(3), (17)(2), (28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g), (30)(1)(f)
8.4.3	(5)(1)(f)
8.5.1	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
8.5.2	(30)(2)(c)
8.5.3	(30)(1)(d)
8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2), (28)(4)
8.5.7	(28)(2), (28)(3)(d)
8.5.8	(28)(2)

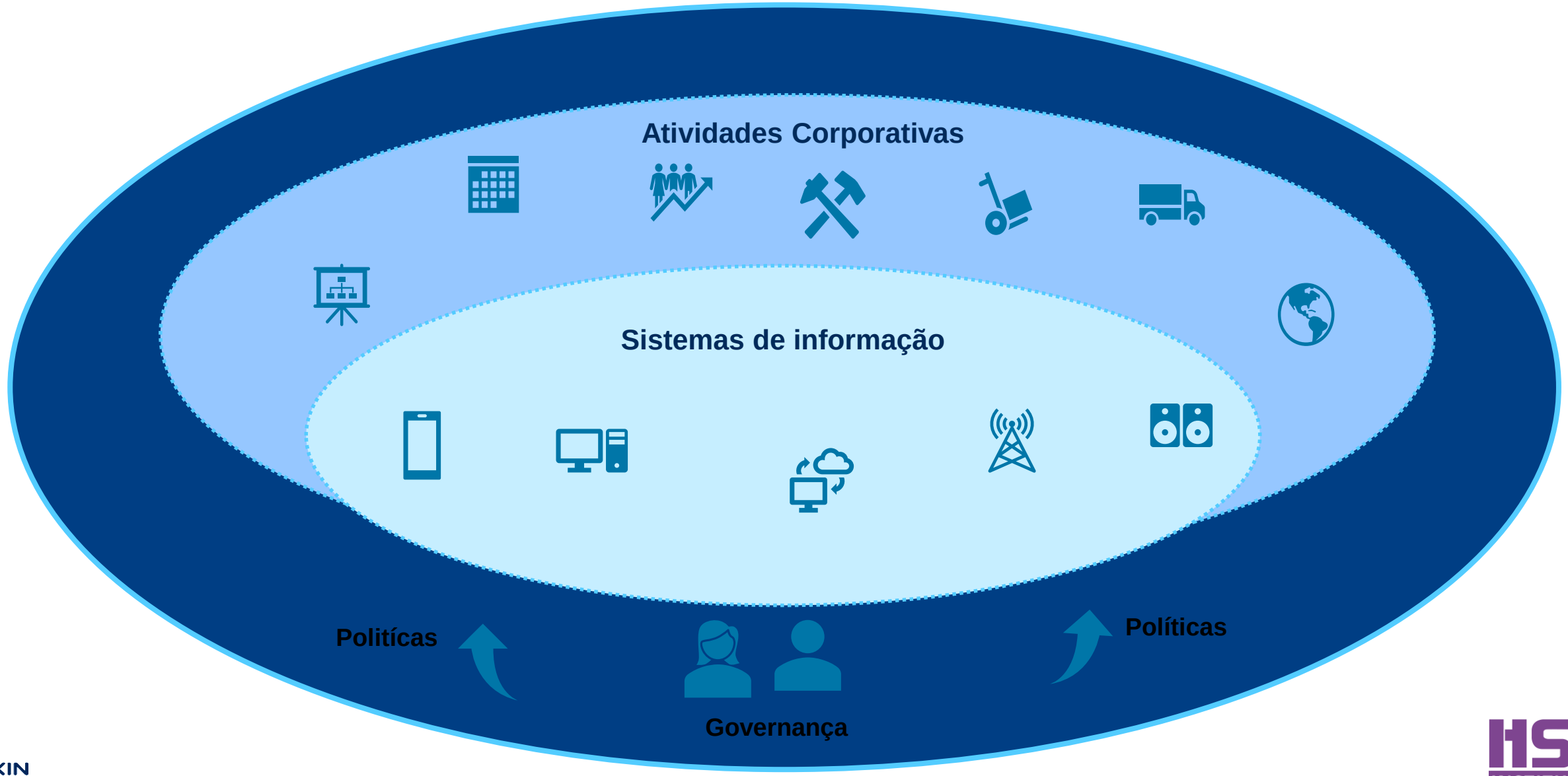
PRIVACY & DATA PROTECTION PRACTITIONER

1. POLÍTICAS DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE



1. POLÍTICAS DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

1. Políticas de Proteção de Dados Pessoais e Privacidade



1. Políticas de proteção de dados pessoais e privacidade
1.1 OBJETIVO DAS POLÍTICAS DE PDP&P

1. Políticas de proteção de dados pessoais e privacidade
1.1 OBEJTIVO DAS POLÍTICAS DE PDP&P
1.1.1 POLÍTICAS E PROCEDIMENTOS

1.1.1 Políticas e Procedimentos necessários em uma organização para cumprir a legislação de proteção de dados pessoais.

O GDPR cita (parte do Considerando nº. 78):

- Para poder demonstrar a conformidade com o presente regulamento, o Controlador deverá adotar políticas internas e aplicar medidas que satisfaçam, em particular, os princípios da proteção de dados pessoais *by design e by default*.
- Essas políticas são "internas" das organizações.

Tipos mencionados no GDPR:

- **Políticas gerais:** a organização declara e tem visões consistentes sobre como pretende atender aos requisitos do GDPR.
- **Políticas de proteção de dados pessoais.**

Outros a considerar:

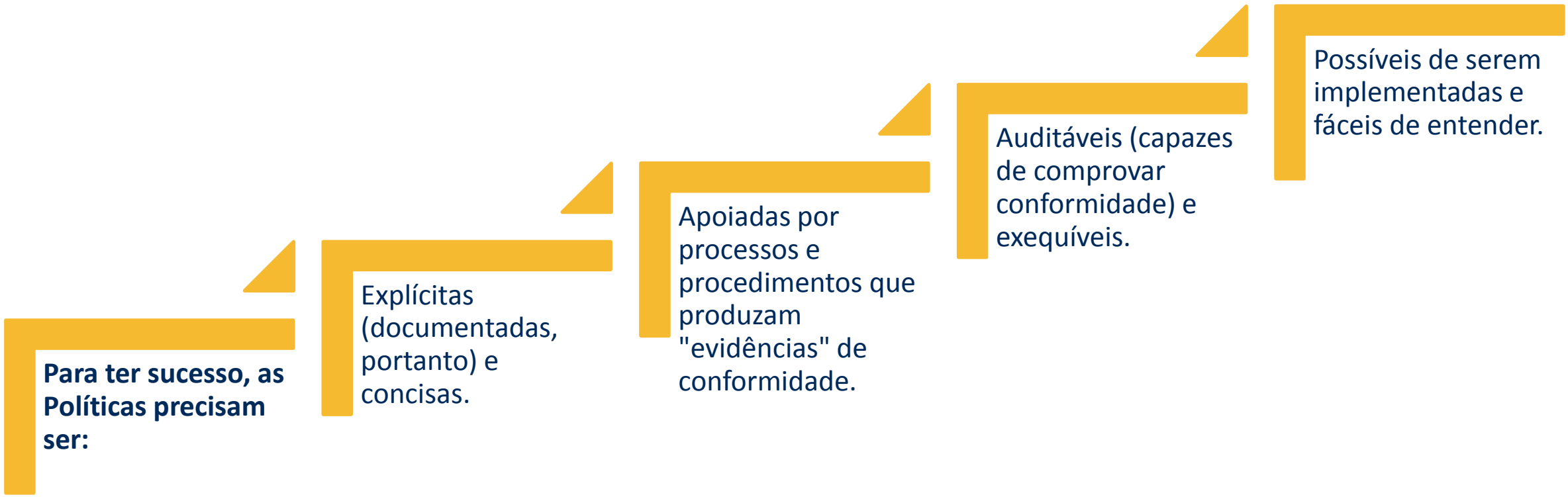
- Política de Privacidade (disponível ao público);
- Política de Segurança da Informação e
- As políticas precisam ser apoiadas por processos e procedimentos, vinculadas às operações da organização e precisam ser auditáveis (para demonstrar conformidade).

1. Políticas de proteção de dados pessoais e privacidade
1.1 PROPÓSITO DAS POLÍTICAS DE PDP&P
1.1.2 CONTEÚDO DAS POLÍTICAS

Políticas devem conter:

- **Objetivo**: pelo menos um descrevendo o que se pretende alcançar e como se relaciona com objetivos empresariais mais amplos;
- **Glossário**: colocar as definições dos principais termos da política;
- **Escopo**: que tópicos e aspectos são cobertos pela política;
- **Público Alvo**: a quem se destina essa política;
- **Aderência e Compliance**: atendimento a requisitos legais, regulatórios e contratuais;
- **Papéis e Responsabilidades**: definições de contatos (funções) e suas responsabilidades (Matriz RACI);
- **Sanções**: consequências em eventual não cumprimento;
- **Referências**: bases para elaboração, por exemplo: normas ISO; Leis ou Regulamentos e
- **Aprovação e Revisão**: controle de versão do documento.

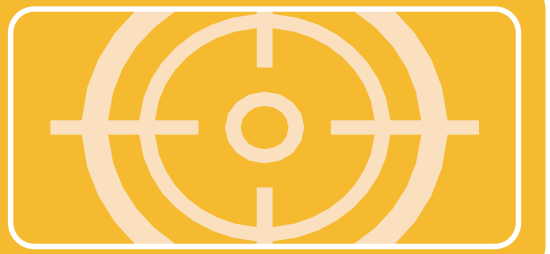
1. Políticas de Proteção de Dados Pessoais e Privacidade
1.1 PROPÓSITO DAS POLÍTICAS DE PDP&P
1.1.2 CONTEÚDO DAS POLÍTICAS



1.1.2.1 O conteúdo das políticas – Exemplo.

Política de Proteção de Dados Pessoais:

Objetivo: O objetivo principal desta política é fornecer diretrizes gerais para as questões de privacidade relacionadas à coleta, uso, processamento, divulgação, monitoramento, etc., dos dados pessoais de uma empresa.



Conteúdo (parcial):

- Objetivo da política;
- Pessoas envolvidas;
- Oportunidade para declinar;
- Coleta de informações pessoais;
- Uso da informação e
- Proteção da informação.

1.1.2.1 O conteúdo das políticas – Exemplo.

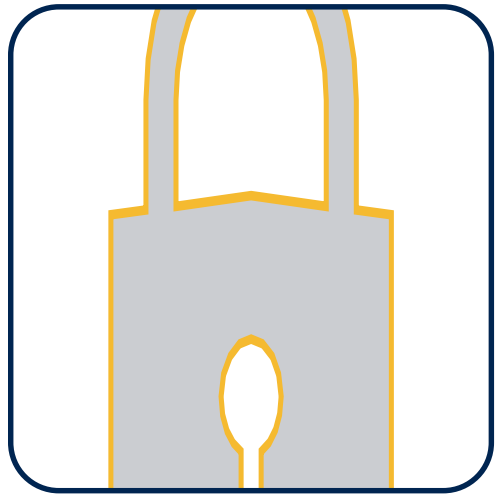
Política de Privacidade:

Objetivo: fornecer ao titular dos dados pessoais, de forma transparente, informações que o tratamento obedece aos princípios do GDPR, tais como, mas não limitado ao período de retenção, aos direitos do titular dos dados, compartilhamento ou não dos dados pessoais com terceiros.

1.1.2.1 O conteúdo das políticas – Exemplos.

Além das políticas de Proteção de Dados Pessoas e de Privacidade, a organização deve determinar quais outras políticas serão pertinentes, de acordo com a sua análise de riscos.

Uma política de segurança da informação em particular seria valiosa. Isso pode incluir **um único documento de política ou uma coleção de políticas diferentes**, nem todas as quais precisarão ser tão prontamente acessíveis aos titulares dos dados quanto à Política de Privacidade.



Os assuntos que podem ser considerados para as políticas de segurança da informação incluem, por exemplo, mas não limitado à:

- Controle de Acesso;
- Classificação da Informação;
- Backup;
- Transferência de Informações;
- Gerenciamento de Vulnerabilidades;
- Criptografia.
- Segurança nas Comunicações;
- Gestão da Cadeia de Suprimentos;
- Etc....

1.1.2.2 Literatura

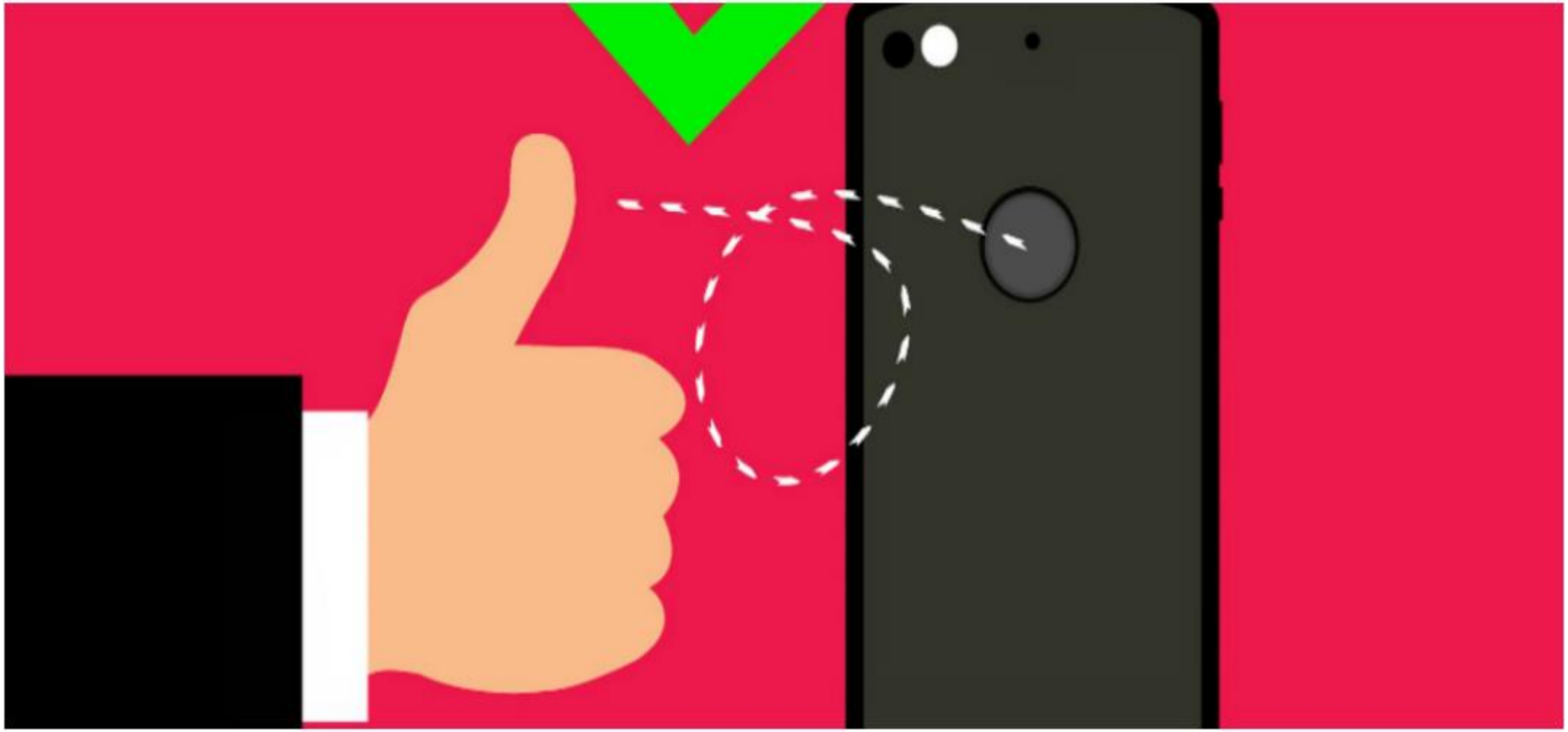
A:

Chapter 16 -*Transitioning and Demonstrating Compliance - § Using policies to demonstrate compliance*.

C:

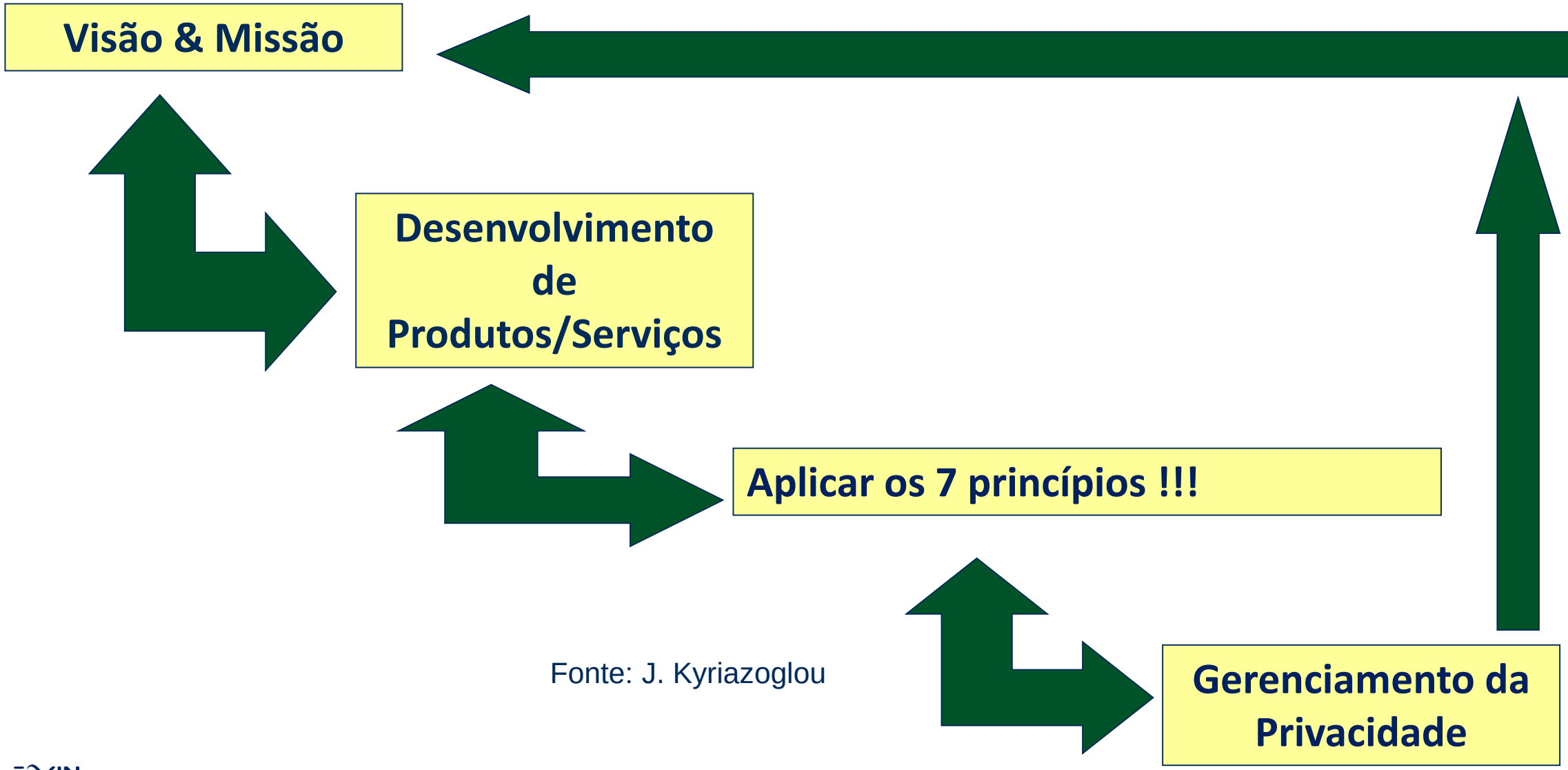
Considerando 53
Considerando 78 (“...políticas internas...”)
Artigo 4º, item 20;
Artigo 13°, nº 1;
Artigo 13°, nº 2;
Artigo 24º, nº 2;
Artigo 19° e
Artigo 39º, nº 1.

1. Políticas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN E BY DEFAULT



Crédito: Pixabay

Proteção de dados pessoais by design e by default



Fonte: J. Kyriazoglou

1. Politicas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN E BY DEFAULT
1.2.1 CONCEITO

***Proteção de dados pessoais by design e by default*:**

A privacidade por *design* avança a visão de que o futuro da privacidade não pode ser assegurado somente pelo cumprimento de marcos regulatórios; em vez disso, a garantia da privacidade deve, idealmente, se tornar o modo de operação padrão de uma organização.

Ao desenvolver e projetar produtos, serviços e aplicativos, os princípios de proteção de dados pessoais por *design* e por *default* **devem** ser observados.

Para poder demonstrar a conformidade com o presente regulamento, o Controlador deverá **adotar políticas internas** e aplicar medidas que satisfaçam, em particular, os princípios da proteção de *dados pessoais by design e by default*. (Considerando 78).

Alguns exemplos de medidas: minimizar o tratamento, pseudonimização, transparência no que diz respeito ao tratamento.

1. Politicas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN BY DEFAULT
1.2.2 OS 7 PRINCÍPIOS!!!!!!!

1 - Proativo e não reativo: proteção antes do fato e não depois.

2 - Proteção de dados pessoais como configuração padrão: O usuário não precisa agir.

3 - Privacidade incorporada ao design: Respeita a performance.

4 - Funcionalidade Total: Privacidade com Segurança**.**

5 - Segurança de ponta a ponta: Proteção total.

6 - Visibilidade e Transparência: Confie, mas verifique**.**

7 - Respeito à privacidade do usuário: Foco e empatia.

1. Políticas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN BY DEFAULT
1.2.3 IMPLEMENTANDO OS 7 PRINCÍPIOS!

Exemplos de desafios para implementação:

Preventiva e não corretiva: • A abordagem tradicional é reativa. Mudar isso requer liderança e mudança cultural. A introdução da arquitetura corporativa pode suportar esse processo.	**Privacidade como configuração *by default***: • Por ex.: emitindo políticas especializadas como 'privilégio mínimo', 'necessidade de conhecimento', 'menos confiança'.	**Privacidade incorporada ao *design***: • Em hardware (por exemplo, TPM) e/ou software (por exemplo, SAMM, CLASP).	**Soma positiva, soma não-zero**: • Conflitos a serem resolvidos: acesso fácil versus acesso seguro, conveniência do usuário versus segurança, simples de implementar versus seguro de usar.	**Proteção completa do ciclo de vida (fim a fim)**: • Requer uma estratégia de segurança que aborde a empresa como um todo. Áreas principais: DBSec e IAM.	**Mantê-la aberta (visível e transparente)**: • Pode ser conseguido, por exemplo, por meio de padrões abertos, avaliação externa e validação, como a auditoria ISO/IEC 27001 e/ou publicação de políticas de segurança.	**Mantê-la centrada no usuário (respeitar o usuário e sua privacidade)**: • Um equilíbrio deve ser alcançado entre a proteção dos dados corporativos e os direitos dos titulares de dados.

1. Politicas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN E BY DEFAULT
1.2.3 IMPLEMENTANDO OS 7 PRINCÍPIOS!

TPM Trusted Party Module:
http:// dpalliance.org.uk/wp-content/uploads/2012/12/1112_Security-by-Design_Trusted_Computing.pdf

SAMM Software Assurance Maturity Model:
https://www.opensamm.org/download/

CLASP Comprehensive, Lightweight Application Security Process:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.9620&rep=rep1&type=pdf

DBSec Database Security:
https://www.brighthub.com/computing/smb-security/articles/61400.aspx

IAM Identity and Access Management:
https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

Privacy by Design and Security by Design

The following table illustrates, at a high level, how a set of Security by Design principles can be modeled upon the 7 Foundational Principles of *Privacy by Design*.

Privacy by Design **Foundational Principles**	**Privacy**	**Security**
	Respect and protect personal information.	Enable and protect activities and assets of both people and enterprises.
1. Proactive not Reactive; Preventative not Remedial	Anticipate and prevent privacy-invasive events *before* they happen. Do not wait for privacy risks to materialize.	Begin with the end in mind. Leverage enterprise architecture methods to guide the proactive implementation of security.
2. Default Setting	Build privacy measures directly into any given ICT system or business practice, by default.	Implement "Secure by Default" policies, including least privilege, need-to-know, least trust, mandatory access control and separation of duties.
3. Embedded into Design	Embed privacy into the design and architecture of ICT systems and business practices. Do not bolt it on after the fact.	Apply Software Security Assurance practices. Use hardware solutions such as Trusted Platform Module.
4. Positive-Sum	Accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a zero-sum approach involving unnecessary trade-offs.	Accommodate all stakeholders. Resolve conflicts to seek win-win.
5. End-to-End Security	Ensure cradle-to-grave, secure lifecycle management of information, end-to-end.	Ensure confidentiality, integrity and availability of all information for all stakeholders.
6. Visibility and Transparency	Keep component parts of IT systems and operations of business practices visible and transparent, to users and providers alike.	Strengthen security through open standards, well-known processes and external validation.
7. Respect for the User	Respect and protect interests of the individual, above all. Keep it user-centric.	Respect and protect the interests of all information owners. Security must accommodate both individual and enterprise interests.

1. Politicas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN E BY DEFAULT
1.2.4 BENEFÍCIOS

PROTEÇÃO *BY DESIGN E BY DEFAULT*	**PRIVACIDADE *BY DESIGN E BY DEFAULT***
MENOR EXPOSIÇÃO AOS RISCOS	RESPEITO AO TITULAR DOS DADOS PESSOAIS
IDENTIFICAÇÃO DE PROBLEMAS NO INÍCIO	MENOS É MAIS!!!!!!
CONSCIENTIZAÇÃO	MENOS INVASIVO
CONFORMIDADE	TRANSPARÊNCIA
??????????????	??????????????

DA METODOLOGIA À POSITIVAÇÃO

1. Politicas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN E BY DEFAULT
1.2.5 EXEMPLO PROTEÇÃO BY DESIGN E BY DEFAULT

PRIVACY COMPANY

Privacy by Design Framework

Governance:
Consists of privacy awareness within the organisation, internal policies, accountability measures, transparency to data subjects, cooperation with third parties and data processors (including data processing agreements)

Subjects / Actions	Anonymisation	1. Data minimisation (art. 5(1)c)	2. Pseudonymisation (art. 4(5))	3. Encryption (art. 6(4)e, 32(1)a)	4. Access control (art. 32(1), 5(1)f)	5. Data protection by default (art. 25(2))	6. Deletion / retention terms (art. 5(1)e)	7. Facilitate rights of data subject (artt. 12-22)
Technical	Anonymise and aggregate (e.g. differential privacy)	Gather only data that is strictly necessary. Delete unnecessary data immediately	Removal of all directly identifying elements, hashing, polymorphic pseudo-id	E.g. public key encryption, disk encryption	Digital data vault, physical access controls, logical access controls, authentication and authorisation	Privacy friendly settings as default setting, transparent user interface, permission management	Automated deletion, 'flagging' of data after end of retention term, sticky policies, data fading	Privacy dashboard, communication / support (art. 5(1)a)
Supportive Documents	No extra measures needed, no personal data involved	Description of purpose of data processing and list of necessary data	Policy for separation of identifying data and other data, agreements	Information security standards (art. 32(1)) and policies	Authorisation matrix and logging, based on need to know and need to access	Registration opt-in / opt-out and permissions	Policy and overview of retention terms, management of e-waste (old documents and devices)	Privacy statement, policy for access requests, correction and deletion of personal data
Alternative	If data is not anonymised follow the scheme	When possible anonymise / aggregate part of the data set, data fading	Other security measures	Other security measures (e.g. stand-alone server)	Access logs, with checks	No alternative, just comply	Anonymise and aggregate (archive if allowed)	No alternative legal obligation

Privacy Audit

A data protection impact assessment can test the requirements and make clear what needs to be done.

The mentioned article numbers refer to the articles of the General Data Protection Regulation (Regulation 2016/679 (GDPR))

www.privacycompany.eu

1. Politicas de Proteção de Dados Pessoais e Privacidade
1.2 PROTEÇÃO DE DADOS BY DESIGN E BY DEFAULT
1.2.6 LITERATURA

Literatura A: Capítulo 5 Seção: Privacidade by design e by default.

Literatura C:

Considerandos 53, 54, 55, 78 e 108.

Artigo 25°.

Artigo 47°, nº 2, Letras b e d.

Literatura adicional

A literatura "A" faz referência a "muitas outras publicações e orientações adicionais ..."; exemplo de tal orientação: Cavoukian, A. & Dixon, M. (2013); Privacidade e segurança por design: uma abordagem de arquitetura empresarial:
https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf

O princípio da proporcionalidade está estabelecido no artigo 5.º do Tratado da União Europeia:

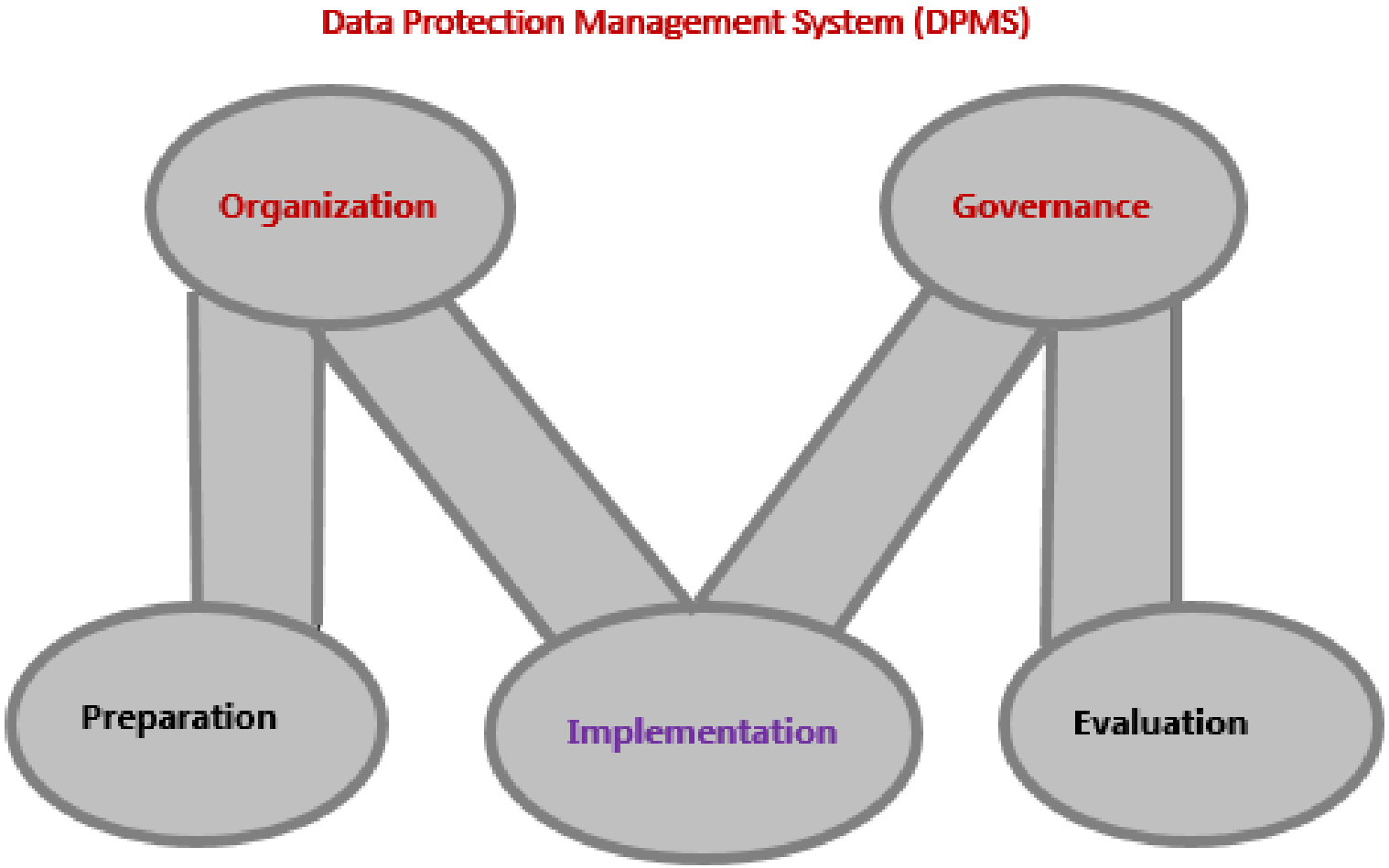
http://eur-lex.europa.eu/summary/glossary/proportionality.html

As ***DPIAs*** são uma parte importante da privacidade *by design e by default*.

PRIVACY & DATA PROTECTION PRACTITIONER

2.GERENCIANDO E ORGANIZANDO A PDP&P

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD



Source: J. Kyriazoglou

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD

2.Gerenciando e Organizando a PDP&P

2.Gerenciando e Organizando a PDP&P

Contextualização do SGPD

O crescente uso das tecnologias de informação e comunicação, juntamente com a Internet, garante que as leis e regulamentos relacionados à proteção, segurança e privacidade de dados pessoais permaneçam importantes e relevantes para todas as empresas e que todas as entidades e organizações em todo o mundo sejam obrigadas a cumpri-las.

A sua empresa deve analisar agora como coletar, gerenciar, armazenar e utilizar os dados pessoais e a melhor forma de cumprir as leis e regulamentos de proteção de dados pessoais e privacidade relevantes, como o GDPR da UE.

A implementação dos controles mais eficazes para resolver os problemas de proteção de dados pessoais é uma tarefa difícil e complexa. Para ajudar, apoiar e permitir que todos da empresa obtenham isso, é necessário **um Sistema de Gestão de Proteção de Dados** para dar suporte a todos. O **SGPD** permite que gerenciem e organizem melhor a proteção de dados pessoais, para que a empresa cumpra os regulamentos de privacidade (como o GDPR da UE) de forma mais eficaz.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD

Literatura A:
Capítulo 12, § Registros de tratamento.
Capítulo 14 Introdução e § Notificação.
Os requisitos descritos nesses capítulos demonstram a importância de um Sistema de Gestão de Proteção de Dados (SGPD).

Literatura B:
Capítulo 2 - SGPD, Item 2.2, Fases do Sistema PDP&P:

- Fase 1: Preparação da Proteção de Dados e Privacidade;
- Fase 2: Organização da Proteção de Dados e Privacidade;
- Fase 3: Desenvolvimento e Implementação da Proteção de Dados e Privacidade;
- Fase 4: Governança da Proteção de Dados e Privacidade e
- Fase 5: Avaliação e Melhoria da Proteção de Dados e Privacidade.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Adicional/Opcional:

Para cada etapa, a literatura contém informações mais detalhadas:

- Todas as atividades para essa etapa;
- Lista de verificação e
- Referência ao GDPR, por exemplo: Princípios de proteção de dados pessoais (Fase 1 / Etapa 2) no Artigo 5° do GDPR.

Essas informações podem ser úteis ao desenvolver exercícios práticos para este curso.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Princípios para tratamento de dados pessoais

1. Lawfull: Fairly and Lawfully;
2. Purpose Specification;
3. Data Relevancy;
4. Data Accuracy;
5. Limited Data Retention;
6. Fair Processing;
7. Accountability; and
8. Transferring personal data overseas.

Fonte: Literatura B, Item 2.2

1. Legalidade: Licitude, Lealdade e Transparência;
2. Limitação da finalidade;
3. Minimização dos dados;
4. Exatidão dos dados;
5. Limitação de Armazenamento;
6. Integridade e Confidencialidade e
7. Responsabilidade.

Fonte: Artigo 5º, GDPR.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Meta: Preparar a organização para à **privacidade**.

Objetivos: Analisar os requisitos de PDP&P e seus impactos; Identificar leis, regulamentos e normas relevantes e estabelecer um Plano de Ação.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Etapas e Ações:

1) Conduzir Análise de Privacidade;
2) Coletar Leis de Privacidade;
3) Analisar o impacto da privacidade para o negócio;
4) Realizar Auditorias e Avaliações iniciais dos dados pessoais;
5) Estabelecer a Organização de Governança de Dados Pessoais;
6) Estabelecer o Fluxo de Dados Pessoais e o Inventário de Dados Pessoais;
7) Estabelecer o programa de PDP&P e
8) Construir Planos de Ação para implementação do SGPD.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 6:

Estabelecer o Fluxo de Dados Pessoais e Inventário de Dados Pessoais.

*** Literatura B:** Apêndice 1: Componentes de um Programa de Proteção de Dados Pessoais e Privacidade.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 6: Estabelecer Fluxo de Dados Pessoais

Se existe!!!!

Onde está???

Como é mantido!!!

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 6: Estabelecer um Inventário de Dados Pessoais

1. Localizar todos os tipos (estruturado e não estruturado);
2. Identificar quem tem a posse do dado pessoal;
3. Identificar os diferentes tipos de dados pessoais;
4. Onde estão os dados pessoais (centralizado ou descentralizado);
5. Responsabilidade e proprietário dos dados pessoais e
6. Estabelecer um processo de atualização do inventário de forma recorrente.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 6: Estabelecer um Inventário de Dados Pessoais

Localizar todos os tipos (estruturado e não estruturado):

- **ESTRUTURADO:**
  - **DADOS DE APLICAÇÃO:**
    - **CRM.**
    - **ERP.**
    - **FINANCIAL.**
    - **MARKETING.**
- **DESESTRUTURADO:**
  - **ARQUIVOS E PASTAS:**
    - **FILE SERVER.**
    - **MOBILE DEVICES.**
    - **LAPTOPS.**

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 6: Estabelecer um Inventário de Dados Pessoais

II. Onde estão os dados pessoais?

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 7: Estabelecer um Programa de PDP&P*

*** Literatura B:** Apêndice 1: Componentes de um Programa de Proteção de Dados e Privacidade.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 7: Estabelecer programa de PDP&P

Empresas e organizações para melhores resultados em relação à proteção de dados pessoais e privacidade, implementam um Programa de Proteção de Dados Pessoais e Privacidade, que é composto por:

- **Plano de Treinamento em Privacidade;**
- **Estratégia de Proteção de Dados Pessoais e Privacidade e**
- **Programa de Proteção de Dados Pessoais e Privacidade.**

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 7: Estabelecer programa de PDP&P

Plano de Treinamento em Privacidade

- Treinamento do DPO;
- Treinamento básico para Todos;
- Treinamento adicional para novas necessidades;
- Integrar treinamento PDP&P com outros treinamentos corporativos;
- Manter um programa de conscientização em PDP&P;
- Manter um programa de certificação em PDP&P e
- Criar indicadores de treinamento e conscientização.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 7: Estabelecer programa de PDP&P

Estratégia de PDP&P:

- Baseada na avaliação de riscos em relação à PDP&P;
- Missão, Valor e Visão em relação à PDP&P;
- Definição do escopo do programa de PDP&P;
- Estabelecer as funções do DPO e
- Detalhamento das estratégias para alcançar as prioridades.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Destacando:
Etapa 7: Estabelecer programa de PDP&P

Programa de PDP&P:

- Enfatizar a missão em relação à PDP&P;
- Identificar os principais objetivos em relação à PDP&P;
- Detalhamento das estratégias e controles em relação à PDP&P e
- Tipos de evidências: Política, Normas, Procedimentos, entre outros.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Entregáveis:

1. Relatório da análise sobre PDP&P (Etapa 1);
2. Manual de Leis de Privacidade (Etapas 2 e 3);
3. Relatório de Auditoria de Dados Pessoais (Etapa 4);
4. Sistema de Fluxo de Dados Pessoais (Etapa 6);
5. Inventário de Dados Pessoais (Etapa 6);
6. Políticas, Normas e Procedimentos de privacidade e proteção de dados pessoais (Etapa 6);
7. Plano de Treinamento de Privacidade (Etapa 7) ;
8. Programa de Privacidade e Proteção de Dados Pessoais (Etapa 7);
9. Budget e Relatório de Organização da Privacidade e Proteção de Dados Pessoais (Etapas 1 a 8) e
10. Planos de Ação de Implementação de P&PD (Etapas 1 a 8).

Resultado: Uma organização preparada para ser mais eficaz em lidar com os riscos de PDP&P e em gerenciá-los para que o impacto nas operações sejam minimizados tanto quanto possível.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.1 FASE 1: PREPARAÇÃO

Literatura B:

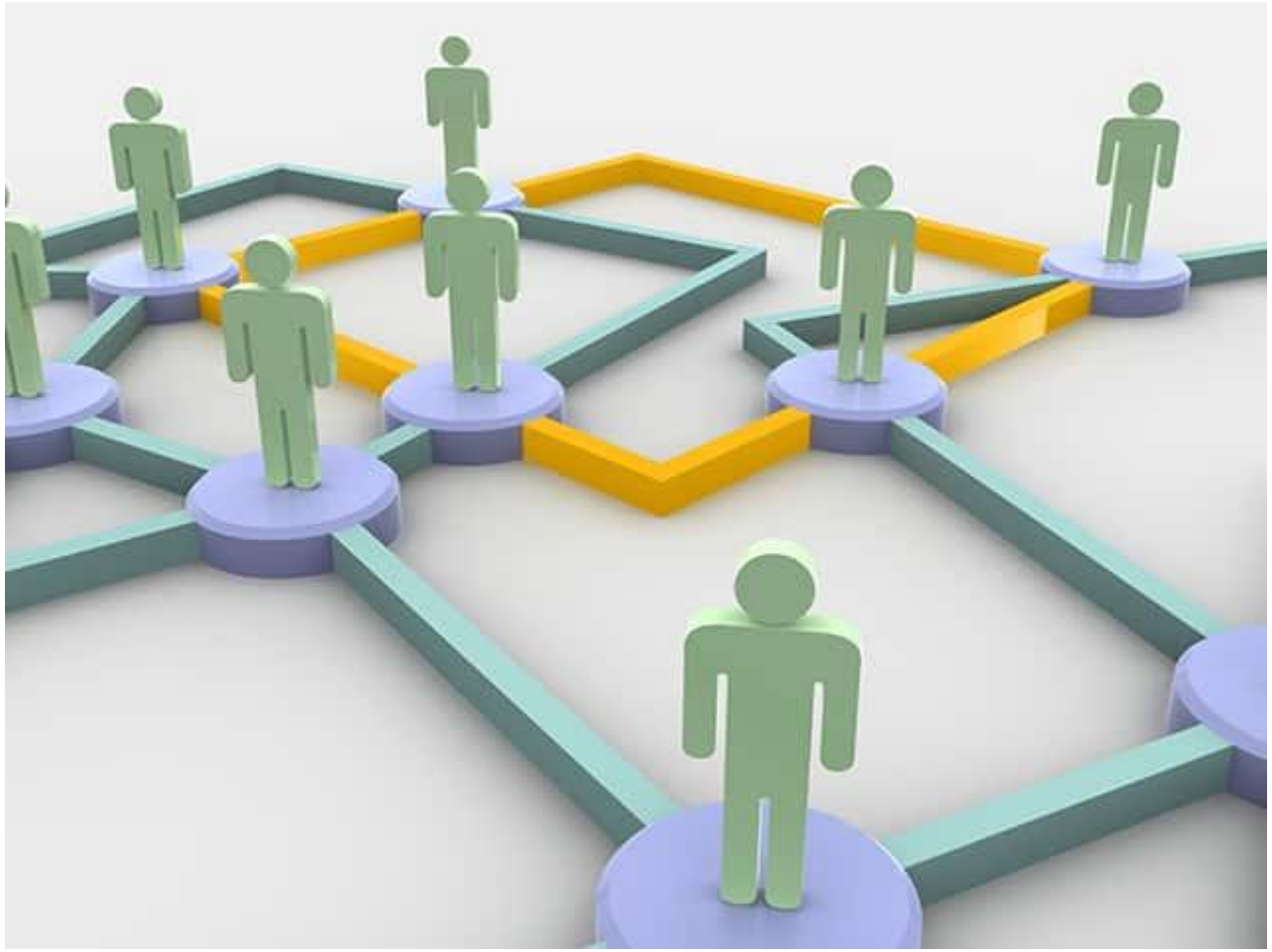
Capítulo 2, Fases do SGPD, Item 2.2.1 - Preparação.

Literatura C:

Em relação ao item 6, Políticas, Normas e Procedimentos recomendamos a leitura de:

- Considerando 53;
- Considerando 78;
- Artigo 4°, item 20;
- Artigo 19°;
- Artigo 24°, n°s 1 e 2;
- Artigo 34°, n° 1, letra b e
- Artigo 39°, n° 1, letra b.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO



2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

Meta: Estabelecer estruturas organizacionais e mecanismos para as necessidades de PDP&P da organização.

Objetivos: Projetar e configurar o programa PDP&P; Nomear um DPO e envolver e obter o compromisso de todas as partes interessadas relevantes.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

Etapas e Ações:

1) Manter um Programa, uma Política de Privacidade de DP e Controles de Governança;
2) Atribuir e manter as responsabilidades em relação à P&PDP;
3) Manter a Alta Direção engajada com a P&PDP;
4) Manter o compromisso de P&PDP;
5) Manter uma comunicação regular sobre problemas de P&PDP
6) Manter engajadas as partes interessadas nas matérias de P&PDP e
7) Implementar e operar o Sistema de P&PDP.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

Destacando:
Etapa 3: Comprometimento da Alta Direção*

*** Literatura B:** Capítulo 2, PD&P, Fases do SGPD, Item 2.2.2.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

Destacando:
Etapa 3: Comprometimento da Alta Direção

Empresas e organizações envolvem a Alta Direção para obter melhores resultados em relação ao SGPD. O **suporte** da Alta Direção pode incluir:

- Patrocinar todas as questões relacionadas à proteção de dados pessoais e privacidade em uma reunião do Conselho de Administração, Presidência, etc.;
- Comunicar a importância da proteção de dados pessoais e privacidade para todos os colaboradores, parceiros e terceiros;
- Participar, **efetivamente**, de iniciativas de proteção de dados pessoais e privacidade e
- Garantir recursos adequados para apoiar as atividades de proteção de dados e privacidade.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

Destacando:
Etapa 7: Sistemas Automatizados para PDP&P

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

Destacando:
Etapa 7: Sistemas Automatizados para PDP&P

- A proteção de dados corporativos é uma das prioridades mais críticas que as organizações enfrentam atualmente;
- Com tantas ameaças em potencial e pontos de entrada, as soluções de proteção de dados precisam ter uma abordagem abrangente e de fim a fim que comece com a identificação de dados valiosos em risco e o planejamento de uma estratégia contínua de proteção de dados que responda a todas as possíveis ameaças - antes mesmo que essas sejam identificadas;
- Isso é resolvido ao projetar as especificações de um sistema informatizado e ferramentas de software para dar suporte ao processo de proteção e privacidade de dados da organização e operá-lo de maneira eficaz e
- Um software de sistema computadorizado para a proteção de dados e privacidade garante a integridade dos dados por vários métodos.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

Destacando:
Etapa 7: Sistemas Automatizados para PDP&P

Exemplos de sistemas automatizados:

- Verificar os arquivos originais e de backup por meio de algoritmos hash;
- Criptografar dados em trânsito e/ou armazenados;
- Fornecer uma interface centralizada de conformidade de gerenciamento de dados;
- Relatórios de sucessos e falhas de backup;
- Gerenciar todos os aspectos do processo de Regras Corporativas Vinculantes e
- Medir e reportar o cumprimento das legislações pertinentes.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.2 FASE 2: ORGANIZAÇÃO

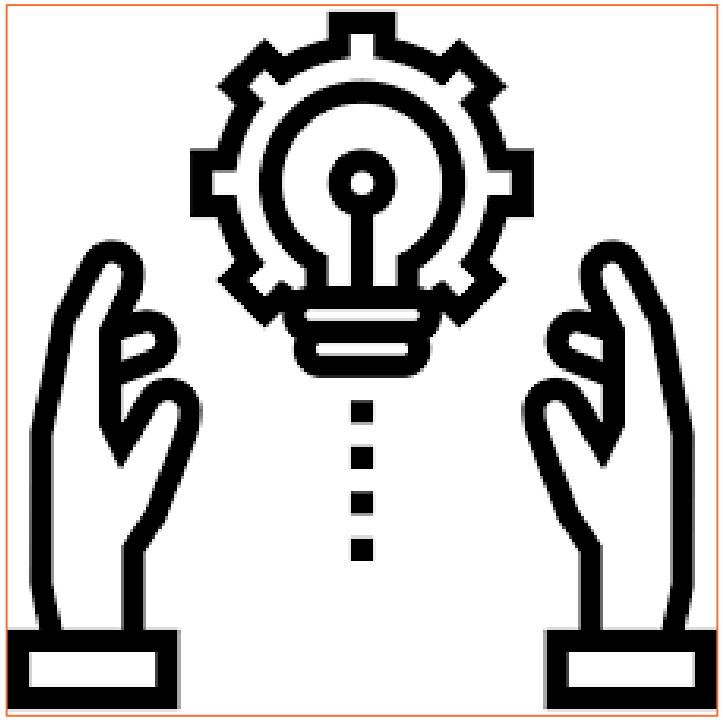
Entregáveis:

1. Estratégia de privacidade e proteção de dados pessoais atualizada (Etapa 1);
2. Programa de privacidade e proteção de dados pessoais atualizado (Etapa 1);
3. Controles de Governança de dados pessoais (Etapa 1);
4. Nomeação do DPO (Etapa 2);
5. Comunicações relacionadas à privacidade e proteção de dados pessoais (Etapas 3, 4, 5 e 6);
6. Rede de privacidade e proteção de dados pessoais (Etapa 4);
7. Privacidade e proteção de dados pessoais informadas nas descrições de trabalho (Etapa 4);
8. Conscientização de privacidade, comunicação e plano de treinamento atualizados (Etapa 5) e
9. Sistema informatizado de privacidade e proteção de dados pessoais (Etapa 7).

Resultado: Estabelecer a estrutura organizacional de PDP&P para uma melhor implantação

Fonte: Literatura B, Capítulo 2, Fases do Sistema PDP&P, Item 2.2.2.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO



Literatura B: Capítulo 2, Fases do Sistema PDP&P / 2.2.3

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Meta: Desenvolver e implementar medidas e controles de PDP&P.

Objetivos: Projetar um sistema de classificação de dados e Desenvolver e implementar Políticas, Procedimentos e Controles.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Etapas e Ações:

1) Desenvolver e implementar estratégias, planos e políticas de PDP&P;
2) Implementar procedimento de aprovados para tratamento de dados pessoais;
3) Registrar bancos de dados de dados pessoais;
4) Desenvolver e implementar um sistema de transferência de dados transfronteiriço;
5) Executar atividades de integração de PDP&P;
6) Executar o Plano de Treinamento de PDP&P e
7) Implementar controles de segurança de dados pessoais.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Destacando:
Etapa 6: Executando o Plano de Treinamento de PDP&P

Empresas e organizações treinam seus funcionários para melhor implementar a proteção de dados pessoais e privacidade em todos os seus programas, sistemas, projetos e funções.

Esse plano inclui as seguintes ações:

1. Realizar treinamento contínuo em privacidade de dados pessoais para o DPO;

2. Executar treinamento básico de privacidade para à equipe;

Continua...

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Destacando:
Etapa 6: Executando o Plano de Treinamento de PDP&P

Continuação:

3. Executar treinamento adicional de privacidade para novas necessidades;

4. Incluir treinamento em privacidade de dados pessoais em outros treinamentos corporativos;

5. Manter a conscientização em privacidade dos dados pessoais;

6. Manter a certificação profissional de privacidade de dados pessoais para o pessoal de privacidade e

7. Medir atividades de conscientização e treinamento sobre privacidade de dados pessoais.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Entregáveis:

1. Sistema de Classificação de Dados Pessoais[1] (Etapa 1);
2. Procedimento para aprovação do Tratamento de Dados Pessoais (Etapa 2);
3. Documento de Registro de Bases de Dados Pessoais (Etapa 3);
4. Implementado o Sistema de Transferência de Dados Transfronteiriço (Etapa 4);
5. Executadas as atividades de integração de PDP&P (Etapa 5);
6. Executadas as atividades de treinamento de PDP&P (Etapa 6) e
7. Implementados os Controles de Segurança de Dados Pessoais (Etapa 7).

Resultado: é desenvolver e implementar um conjunto de métricas de privacidade e proteção de dados pessoais para gerenciar de forma eficaz os dados pessoais em sua organização.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Nota 1: Definições de Classificação da Informação.

Termos e definições de acordo com ISO ABNT NBR 16167/2020:

- **Classificação da informação**: ação de definir o nível de relevância da informação, a fim de assegurar que a informação receba um nível adequado de proteção, conforme seu valor; requisitos legais; sensibilidade e criticidade para à organização.
  - Continua...

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Nota 1: Definições de Classificação de Dados.

Termos e definições de acordo com ISO ABNT NBR 16167/2020:

- **Tratamento da informação**: conjunto de ações referentes ao estabelecimento de diretrizes de proteção da informação em função do seu nível de classificação, envolvendo todas as etapas de seu ciclo de vida.
  - Continua...

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Nota 1: Definições de Classificação de Dados.

Termos e definições de acordo com ISO ABNT NBR 16167/2020:

- **Ciclo de Vida da Informação**: formado pelas seguintes fases: produção; recepção, utilização; acesso; reprodução; transporte; transmissão; distribuição; destinação; arquivamento; armazenamento e eliminação.
  - Continua...

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Nota 1: Definições de Classificação de Dados.

Termos e definições de acordo com ISO ABNT NBR 16167/2020:

- **Criticidade**: nível de crise ou impacto que pode advir da divulgação ou uso indevido da informação;
- **Sensibilidade**: grau de sigilo necessário para informação
  - Continua...

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Nota 1: Definições de Classificação de Dados.

Termos e definições de acordo com ISO ABNT NBR 16167/2020:

- **Proprietário**; responsável por definir a classificação da informação;
- **Custodiante**: responsável por cuidar da manutenção e guarda da informação e
- **Usuário**: pessoa autorizada a interagir com a informação.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.3 FASE 3: DESENVOLVIMENTO/IMPLEMENTAÇÃO

Exemplo de Classificação da Informação:

PÚBLICA: são informações que foram declaradas de conhecimento público por alguém com autoridade para fazê-lo e podem ser disponibilizadas a qualquer pessoa, sem causar possível dano à empresa.

CONFIDENCIAL; contém informações mais importantes e que devem ser protegidas de maneira mais segura. Essas informações incluem: segredos comerciais, programas de desenvolvimento, patentes, material com direitos autorais, possíveis alvos de aquisição e outras informações essenciais para o sucesso da empresa.

RESTRITA: contém todas as outras informações que não são públicas, sensíveis ou confidenciais, como informações armazenadas em arquivos de computador e servidores de rede, listas telefônicas, informações corporativas, etc., que são, no entanto, importantes para atividades do dia a dia da empresa.

SENSÍVEL: contém informações que são mais sensíveis que qualquer outra informação e devem ser protegidas da melhor maneira segura possível. Essas informações incluem dados pessoais extremamente sensíveis, incluindo detalhes de origem racial ou étnica, opiniões políticas pessoais, religião, detalhes sindicais, condições físicas ou mentais, vida sexual, antecedentes criminais, etc.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.4 FASE 4: GOVERNANÇA

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.4 FASE 4: GOVERNANÇA

Meta: Estabelecer mecanismos de governança de PDP&P.

Objetivos: Elaborar e configurar as estruturas de governança de privacidade e proteção de dados pessoais (por exemplo: Programa de PDP&P, DPO, formação do Comitê de PDP&P, etc.), engajar e obter o comprometimento de todas as partes envolvidas com PDP&P e reportar todos os problemas de PDP&P, em busca da melhoria contínua.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.4 FASE 4: GOVERNANÇA

Etapas e Ações:

1) Implementar práticas para gerenciamento de uso de dados pessoais;
2) Manter Avisos de privacidade de dados pessoais;
3) Executar um Plano de Solicitações, Reclamações e Retificações;
4) Executar uma avaliação de riscos de proteção de dados pessoais;
5) Emitir relatórios de PDP&P;
6) Manter documentação de privacidade de dados pessoais e
7) Estabelecer e manter um Plano de Resposta à Violação de Dados Pessoais.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.4 FASE 4: GOVERNANÇA

Entregáveis:

1. Estratégias de PDP&P atualizada (Etapa 1);
2. Políticas de proteção de dados pessoais (Etapa 1);
3. Procedimentos para manter Avisos de privacidade de dados pessoais (Etapa 2);
4. Plano de Solicitações, Reclamações e Retificações (Etapa 3);
5. Processo de avaliação de riscos à proteção de dados pessoais (Etapa 4);
6. Plano de Gestão de Riscos de Terceiros (Etapa 4);
7. Relatórios PDP&P (Etapa 5);
8. Documentação de PDP&P (Etapa 6) e
9. Plano de Resposta à violação de privacidade de dados pessoais (Etapa 7).

Resultado: estabelecer as estrutura de governança de privacidade e proteção de dados pessoais para melhor gestão da PDP&P.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.4 FASE 4: GOVERNANÇA

Destacando:
Entregável 4: Plano de Solicitações, Reclamações e Retificações

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.4 FASE 4: GOVERNANÇA

Destacando:
Entregável 4: Plano de Solicitações, Reclamações e Retificações

Executar as atividades relacionadas ao gerenciamento de solicitações, reclamações e retificações de informações pelos titulares dos dados pessoais mantidos pela empresa. Esse plano contém os seguintes procedimentos:

- Reclamações;

- Oposições em relação ao tratamento;

- Portabilidade;

- Eliminação;

- Manuseio de dados pessoais;

- Acesso a dados pessoais;

- Retificação;

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.4 FASE 4: GOVERNANÇA

Destacando:
Entregável 6: Plano de Gerenciamento de Riscos de Terceiros

Objetivo

Manter contratos e acordos com terceiros (fornecedores) compatíveis com a política de privacidade e proteção de dados pessoais, requisitos legais e ao apetite de risco da empresa.

Conteúdo

Ação nº 1: Realizar a diligência devida para questões de PDP&P para terceiros;

Ação nº 2: Manter os requisitos de PDP&P para terceiros;

Ação nº 3: Manter procedimentos para firmar acordos com terceiros;

Ação nº 4: Manter um processo de avaliação de riscos de PDP&P para terceiros;

Ação nº 5: Realizar a diligência devida em fontes de dados de terceiros;

Ação nº 6: Manter procedimentos para violações de terceiros e

Ação nº 7: Manter a conscientização sobre novos riscos de privacidade de dados pessoais.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.5 FASE 5: AVALIAÇÃO E MELHORIA CONTÍNUA

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.5 FASE 5: AVALIAÇÃO E MELHORIA CONTÍNUA

Meta: Avaliar e melhorar todos os aspectos específicos de PDP&P da organização.

Objetivos: Monitorar a operação e a resolução de todos os assuntos relacionados à privacidade; avaliar regularmente a conformidade com processos e políticas internas e melhorar medidas de proteção de dados pessoais e privacidade.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.5 FASE 5: AVALIAÇÃO E MELHORIA CONTÍNUA

Etapas e Ações:

1) Realizar auditorias internas de PDP&P;
2) Contratar uma parte externa para realizar Avaliações de PDP&P;
3) Realizar avaliações e benchmarks de PDP&P.
4) Executar uma DPIA – Avaliação de Impacto na Proteção de Dados.
5) Resolver os Riscos de PDP&P;
6) Reportar o resultado das Análises de Riscos para PDP&P e
7) Monitorar leis e regulamentos de PDP&P.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.5 FASE 5: AVALIAÇÃO E MELHORIA CONTÍNUA

Destacando:
Etapa 1: Executar auditoria interna

1. O departamento de Auditoria Interna avalia regularmente se a organização está em conformidade com as políticas internas de proteção de dados e privacidade e processos operacionais.
2. Os resultados dessas auditorias e avaliações de privacidade informam e orientam as decisões do departamento de PDP&P para criar ou atualizar políticas, projetar ou adaptar procedimentos, conduzir treinamentos ou participar de outras atividades para minimizar riscos e cumprir requisitos de privacidade internos ou externos.
3. O escopo desta atividade de auditoria de privacidade cobrirá o papel do departamento de PDP&P em participar de auditorias de privacidade e responder a descobertas e realizar auditorias em todos os dados pessoais mantidos em formato eletrônico ou contidos em um sistema de arquivamento manual estruturado.
4. As auditorias são realizadas com base em uma metodologia de auditoria, um programa de auditoria e um conjunto de questionários de proteção e privacidade de dados.

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.5 FASE 5: AVALIAÇÃO E MELHORIA CONTÍNUA

Destacando:
Etapa 1: Executar auditoria interna

Em relação ao Item 3, em particular, mas não exclusivamente, a auditoria cobrirá dados pessoais contidos nos seguintes sistemas e formatos:

- Bases de dados de computadores; Sistemas de gerenciamento de documentos (incluindo documentos armazenados em estruturas de diretório padrão fornecidas por tais instalações); Arquivos de computadores individuais, quando apropriado (por exemplo, planilhas eletrônicas e outras ferramentas de análise, listas processadas por texto etc.); Diretórios de e-mail estruturados; Sistemas de arquivamento manuais estruturados que podem conter dados pessoais; Paginas web; Fotografias; Microficha; Gravações de vídeo/áudio, etc.

Em relação ao Item 4, os questionários no Capítulo 3 da **Literatura B** também podem ser usados nessa tarefa.

Para um exemplo de uma metodologia de auditoria, consulte:

https://global.theiia.org/standards-guidance/topics/documents/201501guidetorbia.pdf

2.Gerenciando e Organizando a PDP&P
2.1 FASES DO SGPD
2.1.5 FASE 5: AVALIAÇÃO E MELHORIA CONTÍNUA

Entregáveis:

1. Relatório de auditoria interna de PDP&P (Etapa 1);
2. Relatório de auditoria externa de PDP&P (Etapa 2);
3. Relatório de avaliação de PDP&P (Etapa 3);
4. Relatório de autoavaliação de PDP&P (Etapa 3);
5. Relatório de benchmark de PDP&P (Etapa 3);
6. Relatório DPIA (Etapa 4);
7. Relatório de riscos resolvidos de PDP&P (Etapa 5);
8. Relatório de resultado da análise de riscos de PDP&P (Etapa 6) e
9. Relatório de monitoramento de leis sobre privacidade (Etapa 7).

Resultado: Auditar os aspectos de privacidade e proteção de dados pessoais e encontrar gaps e erros em métricas e controles implementados e propor ações para as devidas correções.

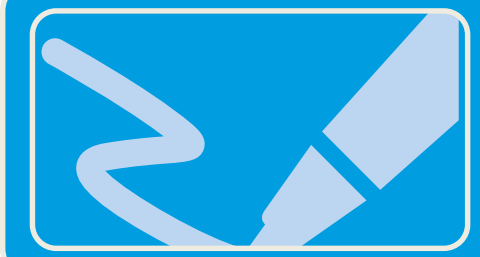
PRIVACY & DATA PROTECTION PRACTITIONER

3. CONTROLADOR, PROCESSADOR E DPO

3. Controlador, Processador e DPO

3. Controlador, Processador e DPO

DPO: Um DPO pode existir tanto para o Controlador (Empresa A), quanto para o Processador (Empresa B).



Instruções escritas: O Controlador fornece instruções escritas ao Processador sobre o tratamento dos dados pessoais de sua responsabilidade.

Controles de Proteção de Dados Pessoais: Tanto o Controlador quanto o Processador projetam e implementam os controles de proteção de dados pessoais apropriados, conforme especificado pelo GDPR.

3. Controlador, Processador e DPO
3.1 PAPÉIS DO CONTROLADOR E PROCESSADOR

Literatura A: Capítulo 12.

Literatura C: Artigo 4° Definições, n°s 7 e 8:

(7) Controlador: pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, **determina os fins e os meios do tratamento de dados pessoais**; Se os fins e os meios desse tratamento forem determinados pela legislação da União ou do Estado-Membro, o Controlador ou os critérios específicos para a sua nomeação podem estar previstos na legislação da União ou do Estado-Membro.

(8) Processador: pessoa física ou jurídica, autoridade pública, agência ou outro organismo **que processa dados pessoais em nome do Controlador.**

3. Controlador, Processador e DPO
3.1 PAPÉIS DO CONTROLADOR E PROCESSADOR
3.1.1 CONTROLADOR

Pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina os fins e os meios do tratamento de dados pessoais. O Controlador detém a responsabilidade final de garantir que os dados pessoais sejam processados de acordo com o GDPR:

- Determinar o objetivo das atividades de tratamento;
- Implementar medidas técnicas e organizacionais para garantir a proteção de dados e demonstrar que o tratamento é realizado de acordo com o GDPR;
- Implementar políticas, normas e procedimentos apropriadas;
- Implementar os princípios de proteção de dados por design e por medidas padronizadas e realizar análises de impacto de proteção de dados;
- Garantir que qualquer Processador cumpra as regras e
- Notificar violações de dados pessoais à autoridade supervisora independente.

3. Controlador, Processador e DPO
3.1 PAPÉIS DO CONTROLADOR E PROCESSADOR
3.1.1 CONTROLADOR

	**Pontos de Atenção:**
	Legalmente responsável não é o mesmo que o responsável em uma matriz RACI.
	O artigo 5 (2) do RGPD estabelece que "O Controlador deve ser responsável em demonstrar conformidade com o parágrafo 1 ('prestação de contas')."
	Portanto, de acordo com o princípio da prestação de contas, o Controlador é responsável pela legalidade do tratamento de dados pessoais.
	A Autoridade Supervisora responsabilizará o Controlador dos dados pessoais sob seus cuidados.
	Se for aplicada uma multa, o Controlador será multado, mesmo se houver contratos escritos entre o Controlador e o Processador.
	O Controlador pode solicitar compensação do Processador se o Processador não cumprir o contrato.

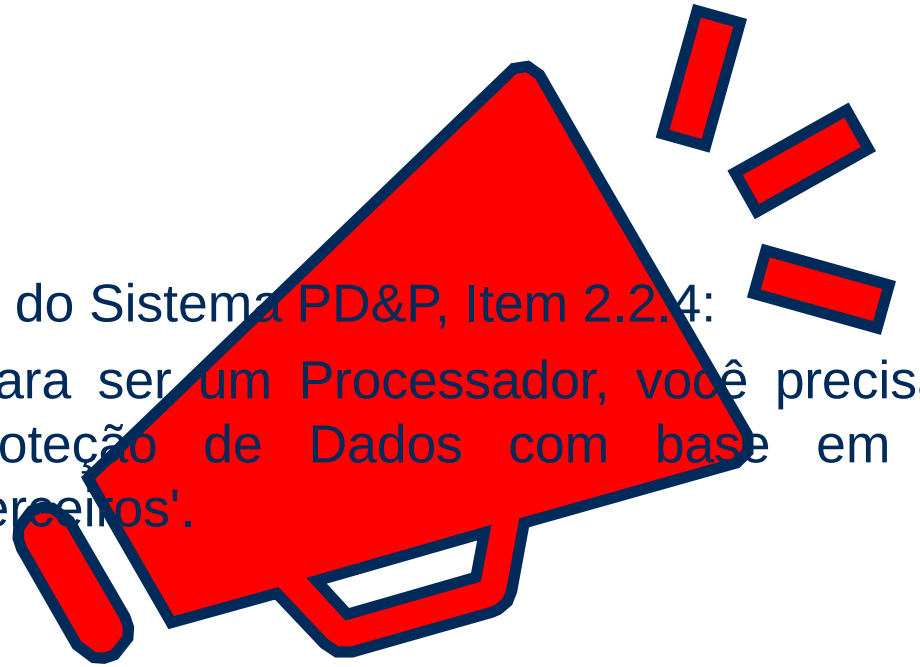
3. Controlador, Processador e DPO
3.1 PAPÉIS DO CONTROLADOR E PROCESSADOR
3.1.2 PROCESSADOR

Pessoa física ou jurídica, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do Controlador:

- Executar apenas as atividades de tratamento 'sob controle' de um Controlador;
- Garantir que as pessoas autorizadas a processar os dados pessoais se comprometeram com a confidencialidade ou estão sob uma obrigação estatutária apropriada de confidencialidade;
- Tomar todas as medidas prescritas no artigo 32° - Segurança do tratamento;
- Se um Processador infringir o regulamento, determinando as finalidades e os meios de tratamento, o Processador será considerado como um Controlador no que diz respeito a esse tratamento e
- Determinar aspectos técnicos e sistemas usados para tratamento, bem como os dados serão armazenados, medidas de segurança, mecanismos de transferência, etc.

3. Controlador, Processador e DPO
3.1 PAPÉIS DO CONTROLADOR E PROCESSADOR
3.1.2 PROCESSADOR

Continuação:



Nota 1.

Literatura B: Capítulo 2, Fases do Sistema PD&P, Item 2.2.4:

Para selecionar um terceiro para ser um Processador, você precisa executar uma Avaliação de Riscos de Proteção de Dados com base em um 'Plano de Gerenciamento de Riscos de Terceiros'.

3. Controlador, Processador e DPO
3.1 PAPÉIS DO CONTROLADOR E PROCESSADOR
3.1.3 CONTROLADOR E PROCESSADOR

O Processador deve:

- Não acionar outro Processador sem autorização prévia específica ou geral por escrito do Controlador;
- Realizar apenas o tratamento que é regido por um contrato ou outro ato jurídico ao abrigo da legislação da União ou de um Estado-Membro, vinculativo para o Processador no que diz respeito ao Controlador;
- Apenas processar dados pessoais em instruções documentadas do Controlador;
- Ajudar o Controlador a adotar as medidas apropriadas;
- Por determinação do Controlador, eliminar ou devolver todos os dados pessoais ao Controlador após o final da prestação de serviços relacionados com o tratamento e
- Disponibilizar ao Controlador todas as informações necessárias para demonstrar conformidade.

Controlador e Processador devem:

- Ambos devem cooperar com a Autoridade Supervisora e apoiar o DPO.

PRIVACY & DATA PROTECTION PRACTITIONER

3.2 DATA PROTECTION OFFICER

3. Controlador, Processador e DPO
3.2 DATA PROTECTION OFFICER
3.2.1 QUANDO UM DPO É OBRIGATÓRIO?

GDPR, Artigo 37º, Designação do DPO:

O tratamento **é realizado por uma autoridade ou organismo público**, com exceção dos tribunais que atuam na sua capacidade judicial (n° 1, alínea a).	**As atividades principais do Controlador ou do Processador consistem em operações de tratamento que**, devido à sua natureza, âmbito e/ou objetivos, requerem uma monitorização regular e sistemática dos dados sujeitos em larga escala (n° 1, alínea b).	**As atividades principais do Controlador ou do Processador consistem no tratamento de uma larga escala de categorias especiais de dados** nos termos do artigo 9°. e dados pessoais relativos a condenações penais e infrações previstas no artigo 10°. (n° 1, alínea c) e	Outros casos que não os mencionados acima ... Quando exigido pela União ou lei do Estado-Membro ... (n° 4).

3. Controlador, Processador e DPO
3.2 DATA PROTECTION OFFICER
3.2.1 QUANDO UM DPO É OBRIGATÓRIO?
3.2.1.1 EXEMPLOS

Hospital: a atividade principal de um hospital é fornecer cuidados de saúde. No entanto, um hospital não poderia fornecer cuidados de saúde com segurança e eficácia sem processar dados de saúde, como registros de saúde dos pacientes. Portanto, o tratamento desses dados deve ser considerado como uma das principais atividades de qualquer hospital, e os hospitais **devem, portanto, designar o DPO.**

Empresa de segurança privada: realiza a vigilância de vários centros comerciais privados e espaços públicos. Vigilância é a atividade principal da empresa, que por sua vez está intrinsecamente ligada ao tratamento de dados pessoais. **Portanto, essa empresa também deve designar um DPO.**

3. Controlador, Processador e DPO
3.2 DATA PROTECTION OFFICER
3.2.1 QUANDO UM DPO É OBRIGATÓRIO?
3.2.1.1 EXEMPLOS

Pequena empresa familiar: ativa na distribuição de eletrodomésticos em uma única cidade usa os serviços de um **Processador,** cuja atividade principal é fornecer serviços de análise de sites e assistência com publicidade e marketing direcionados. As atividades da empresa familiar e de seus clientes não geram tratamento de dados em grande escala, considerando o pequeno número de clientes e as atividades relativamente limitadas. No entanto, as atividades do **Processador**, tendo muitos clientes como essa pequena empresa, em conjunto, estão realizando um tratamento em larga escala. Por consequência, o **Processador deve designar um DPO** ao abrigo do artigo 37°, n° 1, Letra b e ao mesmo tempo, **a empresa familiar não tem a obrigação de designar um DPO.**

3. Controlador, Processador e DPO
3.2 DATA PROTECTION OFFICER
3.2.2 PAPÉIS E RESPONSABILIDADE

O DPO é independente (não recebe instruções sobre o exercício das suas tarefas) e:

- Está envolvido em todas as questões relacionadas com a proteção de dados pessoais;
- Aconselha o Controlador no que diz respeito à DPIA;
- Deve manter seu conhecimento atualizado e especializado;
- Reporta ao mais alto nível de gerenciamento do Controlador;
- É acessível para os titulares de dados e
- Está vinculado por sigilo ou confidencialidade.
  - Continua...

3. Controlador, Processador e DPO
3.2 DATA PROTECTION OFFICER
3.2.2 PAPÉIS E RESPONSABILIDADE

Continuação:

No entanto, o DPO pode realizar outras tarefas, desde que não resulte em conflito de interesses.

Tarefas (principais/obrigatórias):

- Informar e aconselhar o Controlador ou o Processador e os funcionários que realizam o tratamento de suas obrigações em relação ao GDPR;
- Monitorar a conformidade com o GDPR (e qualquer outra legislação nacional relacionada);
- Fornecer orientação quando solicitado, com respeito à DPIA;
- Cooperar com as Autoridade(s) Supervisora(s) e
- Atuar como ponto focal junto à(s) Autoridade(s) Supervisora(s).

3. Controlador, Processador e DPO
3.2 DATA PROTECTION OFFICER
3.2.3 DPO E AS AUTORIDADES SUPERVISORAS

O DPO é a ligação imediata com a Autoridade Supervisora!!!

- *Single point of contact - SPOC*

Obrigações:

Cooperar com a Autoridade Supervisora e

Atuar como ponto de contato com à Autoridade Supervisora, por exemplo:

Para todos os assuntos de tratamento e

Para consulta prévia.

PRIVACY & DATA PROTECTION PRACTITIONER

4. DPIA – Avaliação de impacto sobre a proteção de dados

4. Avaliação de Impacto na Proteção de Dados - DPIA

4. Avaliação de Impacto na Proteção de Dados - DPIA

REQUISITOS GDPR

Fonte: J. Kyriazoglou

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA

Literatura A:

- Capítulo 5: Parágrafo Avaliação de Impacto sobre a Privacidade e Parágrafo Quando conduzir uma DPIA.
- Capítulo 6: Parágrafo DPIAs como parte do gerenciamento de risco.
- Capítulo 8: Parágrafo Objetivos e resultados.

Literatura E: Capítulo 3 Orientações sobre DPIA (WP 248).

Outras referências no GDPR:

- Considerando 84: A fim de reforçar o cumprimento do presente regulamento, o Controlador deverá ser responsável pela realização de uma avaliação de impacto sobre a proteção de dados, a fim de avaliar, em especial, a origem, natureza, especificidade e gravidade desse risco. … Etc...

Continua ...

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA

Considerando 90: … Essa avaliação de impacto deve incluir, em especial, as medidas, as proteções e os mecanismos previstos para reduzir esses riscos, garantir a proteção dos dados pessoais e demonstrar a conformidade com o presente regulamento. … Etc.

O GDPR estabelece as características mínimas de uma DPIA (n.º 7 do artigo 35.º e Considerandos 84 e 90):

- -"uma descrição das operações de tratamento previstas e as finalidades do tratamento";
- - "uma avaliação da necessidade e proporcionalidade do tratamento";
- - "uma avaliação dos riscos para os direitos e liberdades dos titulares de dados";
- - "as medidas previstas para:
  - "Abordar os riscos";
  - "Demonstrar o cumprimento do presente regulamento".

Função DPO:

Artigo 39.º Funções do encarregado da proteção de dados, n° 1, alínea c: **Prestar aconselhamento**, se tal for solicitado, no que diz respeito à avaliação de impacto sobre a proteção de dados, e acompanhar o seu desempenho nos termos do artigo 35.º.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS

<u>Condições obrigatórias</u>: (Art. 35°, Item 3, letras 'a', 'b' e 'c'):

- No caso de uma avaliação sistemática e abrangente dos aspectos pessoais relativos a pessoas físicas, baseada no tratamento automatizado, incluindo a criação de perfis;
- No caso de tratamento em grande escala de categorias especiais de dados ou dados pessoais relacionados a condenações e delitos e
- No caso de um acompanhamento sistemático de uma área de acesso público em grande escala.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS

Os seguintes critérios que devem ser considerados:

- 1. Avaliação ou pontuação (score, rating, etc.....).

Referência: Considerandos 71 e 91.

- 2. Tomada de decisão automatizada com efeito legal ou similar significativo.

Referência: Artigo 35°, (3), (a).

- 3. Monitoramento sistemático.

Referência: Artigo 35°, (3), (c).

- 4. Dados pessoais sensíveis.

Referência: Artigo 35°, (3), (b).

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS

5. Dados processados em larga escala:

Referência: O GDPR não define o que constitui grande escala, embora o Considerando 91 forneça alguma orientação. Em qualquer caso, o Grupo de Trabalho do Artigo 29.° recomenda que os seguintes fatores, em especial, sejam considerados quando se determina se o tratamento é ou não efetuado em grande escala:

A. O número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;

B. O volume de dados e/ou a diversidade de dados diferentes a tratar;

C. A duração, ou permanência, da atividade de tratamento de dados;

D. A extensão geográfica da atividade de tratamento.

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS

Continuação:

Os seguintes critérios devem ser considerados:

6. Conjuntos de dados que foram equiparados ou combinados.
   Referência: WP 248, Item III - DPIA: uma explicação do regulamento, Nº. 6.
7. Dados relativos a titulares de dados vulneráveis.
   Referência: WP 248, Item III - DPIA: uma explicação do regulamento, Nº. 7.
8. Uso inovador ou aplicação de soluções tecnológicas ou **organizacionais**.
   Referência: Artigo 35° (1) e Considerandos 89 e 91.
9. Transferência de dados pessoais para fora da União Europeia.
   Referência: Considerando 116.

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS

Continuação

Os seguintes critérios devem ser considerados:

10. Quando o tratamento em si "impede que os titulares de dados exerçam um direito ou utilizem um serviço ou um contrato".

    Referência: Artigo 22º e Considerando 91. Estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que esses celebrem um contrato. Um exemplo disso é quando um banco faz um controle seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário com vista a decidir se lhes concede ou não um empréstimo.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS
4.1.1.1 OBRIGATORIEDADE

Literatura E, Capítulo III:

"A realização de uma DPIA é obrigatória apenas quando o tratamento" possa resultar em um **alto risco** aos direitos e liberdades das pessoas físicas (Artigo 35° (1), ilustrado pelo Artigo 35° (3) e complementado pelo Artigo 35° (4))".

É particularmente relevante quando uma nova tecnologia de tratamento de dados está sendo introduzida.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS
4.1.1.1 OBRIGATORIEDADE

Caso 1:

Um hospital processando os dados genéticos e de saúde de seus pacientes (sistema de informações hospitalares).

Critérios:

(1) Dados sensíveis,

(2) Dados relativos a titulares de dados vulneráveis.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS
4.1.1.1 OBRIGATORIEDADE

Caso 2:

O uso de um sistema de câmeras para monitorar o comportamento de condução em autoestradas. O Controlador prevê a utilização de um sistema inteligente de análise de vídeo para destacar carros e reconhecer automaticamente as placas.

Critérios:

(1) Monitoramento sistemático,

(2) Uso inovador ou aplicação de soluções tecnológicas ou organizacionais.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.1.1 APLICANDO OS CRITÉRIOS
4.1.1.1 OBRIGATORIEDADE

Caso 3:

Uma empresa que monitora as atividades de seus funcionários, incluindo o monitoramento da estação de trabalho dos funcionários, a atividade na Internet, etc.

Critérios:

(1) Monitoramento sistemático

(2) Dados relativos a sujeitos de dados vulneráveis.

4. Avaliação de Impacto na Proteção de Dados – DPIA

4.1 CRITÉRIOS PARA À DPIA

4.1.1 APLICANDO OS CRITÉRIOS

4.1.1.2 NÃO OBRIGATORIEDADE

Literatura E, Capítulo III, letra 'b':

A DPIA não é exigida nos seguintes casos:

- quando o tratamento não for "suscetível de resultar num risco elevado para os direitos e liberdades de pessoas físicas" (Artigo 35° (1));

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA

4.1 CRITÉRIOS PARA À DPIA

4.1.1 APLICANDO OS CRITÉRIOS

4.1.1.2 NÃO OBRIGATORIEDADE

Literatura E, Capítulo III, letra 'b':

A DPIA não é exigida nos seguintes casos:

- quando a natureza, âmbito, contexto e finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada uma DPIA. Nesses casos, podem ser utilizados os resultados da DPIA realizada para o tratamento semelhante (Artigo 35° (1));

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA

4.1 CRITÉRIOS PARA À DPIA

4.1.1 APLICANDO OS CRITÉRIOS

4.1.1.2 NÃO OBRIGATORIEDADE

Literatura E, Capítulo III, letra 'b':

A DPIA não é exigida nos seguintes casos:

sempre que uma operação de tratamento tenha uma base legal na legislação da UE ou dos Estados-Membros e tenha declarado que não é necessário efetuar uma DPIA inicial, quando a lei regula a operação específica de tratamento e onde uma DPIA, de acordo com as normas do GDPR, já foi realizado como parte do estabelecimento dessa base jurídica (Artigo 35° (10));

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA

4.1 CRITÉRIOS PARA À DPIA

4.1.1 APLICANDO OS CRITÉRIOS

4.1.1.2 NÃO OBRIGATORIEDADE

Literatura E, Capítulo III, letra 'b':

- Quando as operações de tratamento tiverem sido previamente controladas por uma autoridade supervisora antes de Maio/2018, em condições específicas que não se tenham alterados (Item III, letra C);

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA

4.1 CRITÉRIOS PARA À DPIA

4.1.1 APLICANDO OS CRITÉRIOS

4.1.1.2 NÃO OBRIGATORIEDADE

Literatura E, Capítulo III, letra 'b':

quando uma operação de tratamento, nos termos do artigo 6º, nº 1, alíneas c) ou e), tiver um fundamento jurídico no direito da UE ou de um Estado-Membro, em que o direito regule a operação de tratamento específica e em que a DPIA já tenha sido realizada como parte da adoção desse fundamento jurídico (artigo 35º, nº 10), salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tratamento);

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA

4.1 CRITÉRIOS PARA À DPIA

4.1.1 APLICANDO OS CRITÉRIOS

4.1.1.2 NÃO OBRIGATORIEDADE

Literatura E, Capítulo III, letra 'b':

quando o tratamento estiver incluído na lista opcional (definida pela autoridade supervisora) de operações de tratamento para as quais não é obrigatória uma DPIA (artigo 35º, nº 5)

Continua...

4. Avaliação de Impacto na Proteção de Dados – DPIA

4.1 CRITÉRIOS PARA À DPIA

4.1.1 APLICANDO OS CRITÉRIOS

4.1.1.2 NÃO OBRIGATORIEDADE

Revista online:

usando uma lista de endereços para enviar um resumo diário genérico para seus assinantes.

Critérios: Nenhum.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.2 OBJETIVOS E RESULTADOS

Objetivos:

- Identificar riscos específicos aos dados pessoais como resultado das atividades de tratamento e o foco está na privacidade e proteção de dados pessoais;
- Analisar como programas, funções, sistemas e processos coletam, usam, compartilham e mantêm dados pessoais para garantir a conformidade com as leis e políticas de proteção de dados pessoais/privacidade aplicáveis e
- Determinar os riscos aos dados pessoais inerentes aos programas, sistemas, funções, projetos e processos.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.1 CRITÉRIOS PARA À DPIA
4.2 OBJETIVOS E RESULTADOS

Resultados

- Uma descrição do tratamento e seus propósitos/finalidades.
- Os interesses legítimos que você está buscando com esse tratamento.
- Uma avaliação da necessidade e proporcionalidade do tratamento.
- Uma avaliação dos riscos para os direitos e liberdades dos titulares desses dados pessoais.
- As medidas previstas para mitigar os riscos.
- Todas as proteções e medidas de segurança para demonstrar o cumprimento do Regulamento.
- Indicações de prazos se o tratamento incluir a exclusão de dados pessoais.
- Uma indicação de qualquer proteção de dados *by design* e *by default*.
- Uma lista dos destinatários de dados pessoais.
- Conformidade com códigos de conduta aprovados e
- Informações se os titulares dos dados pessoais foram consultados e se consentiram.

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.2 ETAPAS DA DPIA
4.2.1 AS ETAPAS DE UMA DPIA

1) Identificar a necessidade de uma DPIA;

2) Descrever os fluxos de informação;

3) Identificar os riscos de privacidade e afins;

4) Identificar e avaliar soluções de privacidade;

5) Assinar e registrar os resultados;

6) Integrar os resultados em um plano de projeto e

7) Consultar as partes interessadas internas e externas.

Source: enisa.europa.eu

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.2 ETAPAS DA DPIA
4.2.1 AS ETAPAS DE UMA DPIA

Alguns exemplos de riscos para dados pessoais:

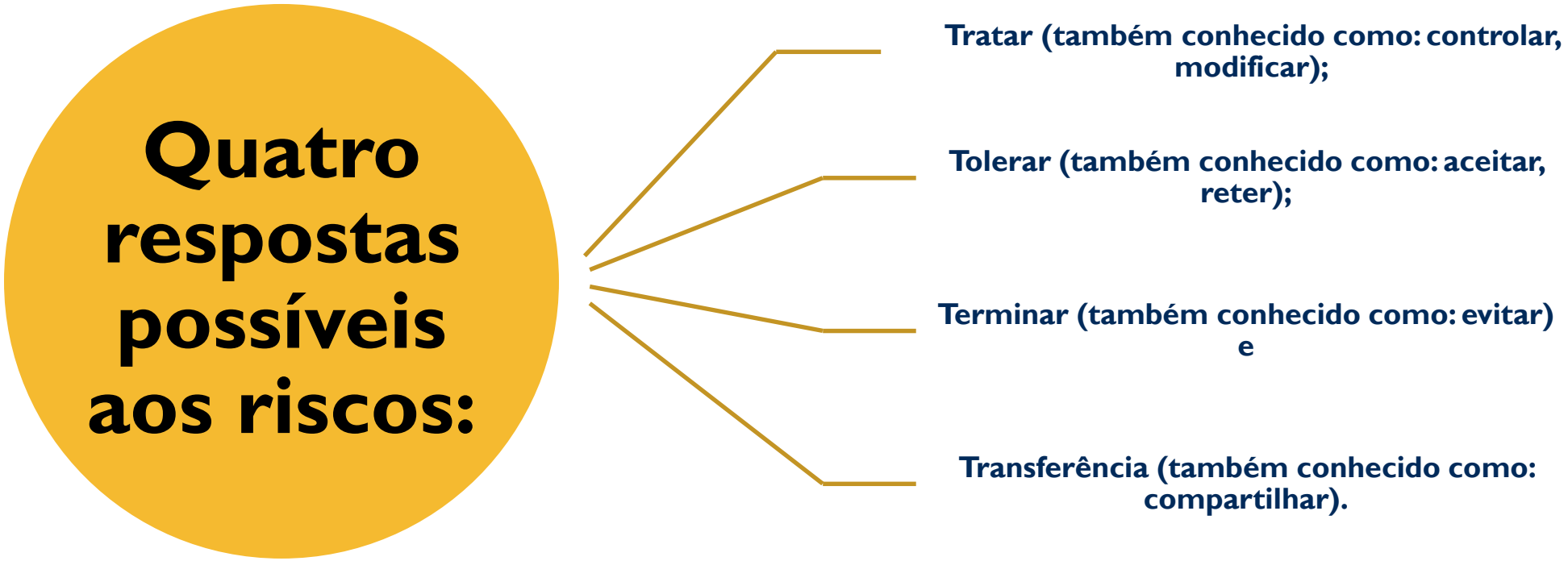
Hacking, malwares, roubo ou danos a dados pessoais; *phishing*, **falta de treinamento ,** dados não criptografados em equipamentos móveis, controle de acesso inadequado, senhas fracas, etc.

Podemos ainda considerar a existência de vários riscos relacionados às seguintes <u>questões críticas</u> no tocante à proteção de dados pessoais:

- Limitação da finalidade; Minimização dos dados; Informações e direitos de acesso; Base legal para tratamento e transferência; Retificação e Exclusão; Qualidade e Exatidão; Segurança dos dados pessoais; Compartilhamento; Retenção e Responsabilidade.

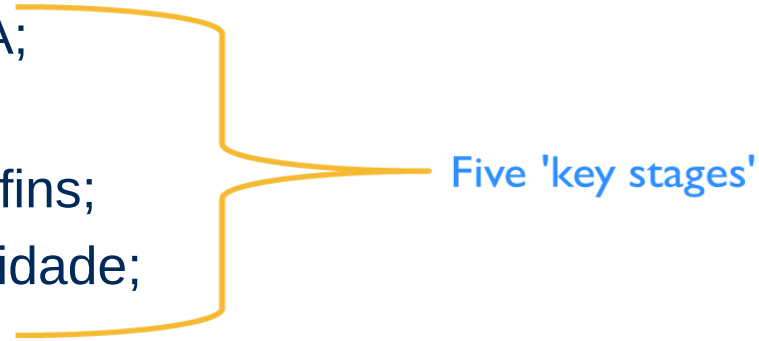
4. Avaliação de Impacto na Proteção de Dados – DPIA
4.2 ETAPAS DA DPIA
4.2.1 AS ETAPAS DE UMA DPIA

4. Avaliação de Impacto na Proteção de Dados – DPIA
4.2 ETAPAS DA DPIA
4.2.1 AS ETAPAS DE UMA DPIA



4. Avaliação de Impacto na Proteção de Dados – DPIA
4.2 ETAPAS DA DPIA
4.2.1 AS ETAPAS DE UMA DPIA

- **Os sete passos:**
  1. Identificar a necessidade de uma DPIA;
  2. Descrever os fluxos de informação;
  3. Identificar os riscos de privacidade e afins;
  4. Identificar e avaliar soluções de privacidade;
  5. Assinar e registrar os resultados;
  6. Integrar os resultados em um plano de projeto e
  7. Consultar as partes interessadas internas e externas.



- Consulta das partes interessadas:
  - Partes interessadas internas: equipes de projeto, DPO, jurídico, compras, equipe de TI, etc.
  - Partes interessadas externas: titulares de dados, especialista em segurança da informação, autoridade supervisora, etc.

PRIVACY & DATA PROTECTION PRACTITIONER

5. VIOLAÇÃO DE DADOS PESSOAIS, NOTIFICAÇÃO E RESPOSTA A INCIDENTES

Ciclo de Vida da Violação de Dados Pessoais

Framework de Governança Corporativa

Source: J. Kyriazoglou

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.1 DEFINIÇÃO DE VIOLAÇÃO DE DADOS

Artigo 4º - Definições, Item 12: Uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.1 DEFINIÇÃO DE VIOLAÇÃO DE DADOS

5.1.1 QUANDO OCORRE

- Incidente → Incidente de segurança (evento de seg. da informação) → Violação de dados.
- **Violação de dados pessoais** significa uma quebra de segurança, de modo acidental ou ilícito, que leva à:
  - Destruição;
  - Perda;
  - Alteração;
  - Divulgação ou acesso não autorizados;

  de/para **dados pessoais** transmitidos, armazenados ou processados de qualquer outra forma.

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.1 NOTIFICAÇÃO À AS

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.1 NOTIFICAÇÃO À AS

O quê?

- O Controlador deve documentar quaisquer violações de dados pessoais, compreendendo os fatos relativos à violação de dados pessoais, os seus efeitos e as medidas corretivas adotadas - Art. 33°, n° 5.

Quando?

- **O Processador** deve, sem demora indevida após tomar conhecimento de uma violação de dados pessoais, notificar o Controlador - Art. 33°, n° 2.
- **O Controlador** deve, sem demora indevida após tomar conhecimento de uma violação de dados pessoais, notificar à Autoridade Supervisora em até 72 horas após ter tomado conhecimento disso - Art. 33°, n° 1.

Quando não?

- Quando é improvável que a violação de dados pessoais resulte em risco para os direitos e liberdades das pessoas físicas - Art. 33°, n° 1.
  - **Continua..**

5. Violação de Dados Pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.1 NOTIFICAÇÃO À AS

Como elaborar uma notificação?

Uma notificação deve conter, ao menos:

- A natureza da violação de dados pessoais, incluindo: categorias e número aproximado de titulares de dados e registros de dados afetados;
- Nome e detalhes de contato do DPO (ou outro contato);
- As consequências prováveis da violação de dados pessoais e
- Medidas tomadas e/ou propostas para mitigação da violação (incluindo aquelas para mitigar possíveis efeitos adversos).

Artigo 33°, n° 4 - Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, essas podem ser fornecidas por fases, sem demora injustificada.

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.2 NOTIFICAÇÃO AO TITULAR DOS DADOS

5. Violação de Dados Pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.2 NOTIFICAÇÃO AO TITULAR DOS DADOS

Quando apresentar?

- Se é provável que a violação de dados pessoais resulte em **risco elevado** para os direitos e liberdades das pessoas físicas.

Quando não apresentar?

- Se o Controlador implementou medidas que impedem que os dados pessoais sejam lidos por pessoas não autorizadas (por exemplo, criptografia);
- Se o Controlador tiver tomado medidas para garantir que o 'alto risco' não se materialize;
- Se a notificação da pessoa em causa implicasse um esforço desproporcionado (por exemplo, um elevado número de titulares de dados; nesse caso, uma comunicação pública seria considerada uma "forma igualmente eficaz");

Continua...

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.2 NOTIFICAÇÃO AO TITULAR DOS DADOS

Continuação:

Como elaborar uma notificação ao(s) titular(es) dos dados pessoais?

- Em linguagem clara e simples;
- Em estreita cooperação com a Autoridade Supervisora;
- Notificação deve conter, ao menos:
  - Nome e detalhes de contato do DPO (ou outro contato);
  - As prováveis consequências da violação de dados pessoais e
  - As medidas tomadas ou propostas para lidar com a violação de dados pessoais (incluindo aquelas para mitigar possíveis efeitos adversos).

5. Violação de Dados pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.2 NOTIFICAÇÃO AO TITULAR DOS DADOS

Continuação:

"A Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) elaborou recomendações para uma metodologia de avaliação da gravidade de uma violação, na qual os Controladores ou Processadores podem considerar útil na elaboração do seu plano de resposta para a gestão de violações de dados pessoais".

Fonte: https://www.enisa.europa.eu/publications/dbn-severity

5. Violação de Dados Pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.2 NOTIFICAÇÃO AO TITULAR DOS DADOS

Caso:

Notificação do Titular dos Dados em caso de violação de dados pessoais e medidas propostas

Caso:
Notificação do Titular dos Dados em caso de violação de dados pessoais e medidas propostas

Violação de dados pessoais:
Ataque via ransomware.
Efeitos nos dados pessoais: Algum dado pessoal foi roubado ou danificado.
Medidas atuais
1. Backup em 2 locais;
2. Anti-malware;
3. Monitoramento de segurança e
4. Firewalls.
Novas medidas propostas, a serem tomadas:
1. Treinar pessoal em técnicas de engenharia social.
2. Bloqueio de endereços IP e sites maliciosos conhecidos.

5. Violação de Dados Pessoais, Notificação e Resposta a Incidentes

5.2 REQUISITOS PARA NOTIFICAÇÃO

5.2.3 INFORMAÇÕES OBRIGATÓRIAS

Existe uma obrigação geral de manter registros de atividades de tratamento;

O Controlador documentará quaisquer violações de dados pessoais, incluindo:

1) Os fatos relacionados com a violação de dados pessoais, natureza, categorias e número de dados e titulares desses dados;
2) O nome e detalhes de contato do DPO ou ponto focal junto à AS;
3) Seus efeitos (consequências) e
4) As ações corretivas e medidas tomadas.

O Controlador deve documentar quaisquer violações de dados pessoais:

- Essa documentação deve permitir à Autoridade Supervisora verificar a conformidade com o artigo 33°, Notificação de uma violação de dados pessoais à Autoridade Supervisora.

PRIVACY & DATA PROTECTION PRACTITIONER

6. ATIVIDADES PRÁTICAS

6. Atividades Práticas

6.1 PAPÉIS E RESPONSABILIDADES: CONTROLADOR, PROCESSADOR E DPO

6.2 DPIA

6.3 VIOLAÇÃO DE DADOS PESSOAIS

Obrigado!

O foco do HSI é sempre a melhoria contínua desse conteúdo. Por isso, criamos esse canal direto com você. Aponte sua câmera para esse QR code, acesse nossa pesquisa de satisfação e conte pra gente o que achou e onde podemos melhorar.