Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Mapeando práticas de privacidade ao CIPL Accountability Framework

GT de Proteção de Dados da ABES - Associação Brasileira das Empresas de Software

Giovanna Carloni | 09 de Junho de 2020

Uma Reflexão Inicial

Se você está implementando privacidade e proteção de dados somente para fins de compliance, você já falhou.

Privacidade e proteção de dados são uma responsabilidade ética e um imperativo de negócios.

Harvey Jang, Vice President & Chief Privacy Officer, Cisco

Estrutura da Apresentação

Contexto
A motivação do CIPL e os objetivos do projeto

Metodologia
Usada para coletar informações e redigir o relatório

Mapeamento
E estudos de caso sobre accountability organizacional na proteção de dados

Sobre o CIPL

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Think Tank Global de Privacidade e Cybersecurity

BRIDGING REGIONS | BRIDGING INDUSTRY & REGULATORS | BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

90+
Member companies

5+
Active projects & initiatives

20+
Events annually

15+
Principals and Advisors

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

We **SHAPE** privacy policy, law and practice

We **CREATE** and implement best practices

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age

Twitter.com/the_cipl
https://www.linkedin.com/company/centre-for-information-policy-leadership
www.informationpolicycentre.com
2200 Pennsylvania Ave NW Washington, DC 20037
Park Atrium, Rue des Colonies 11 1000 Brussels, Belgium
30 St Mary Axe London EC3A 8EP

CIPL Accountability Framework

Organisations must be able to demonstrate accountability – internally and externally

Accountability is not static, but dynamic, reiterative and a constant journey

Accountability requires comprehensive privacy programmes that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls

Company values and business ethics shape accountability

Definindo Accountability na Proteção de Dados

Accountability is globally recognised as a key building block for effective data privacy regulation and its corresponding implementation. It means that organisations:

1

Take steps such as implementing a comprehensive data privacy management programme (DMPM) to translate data privacy legal requirements into risk-based, concrete, verifiable and enforceable actions and controls relating to the processing of personal data which are reviewed and adapted over time

2

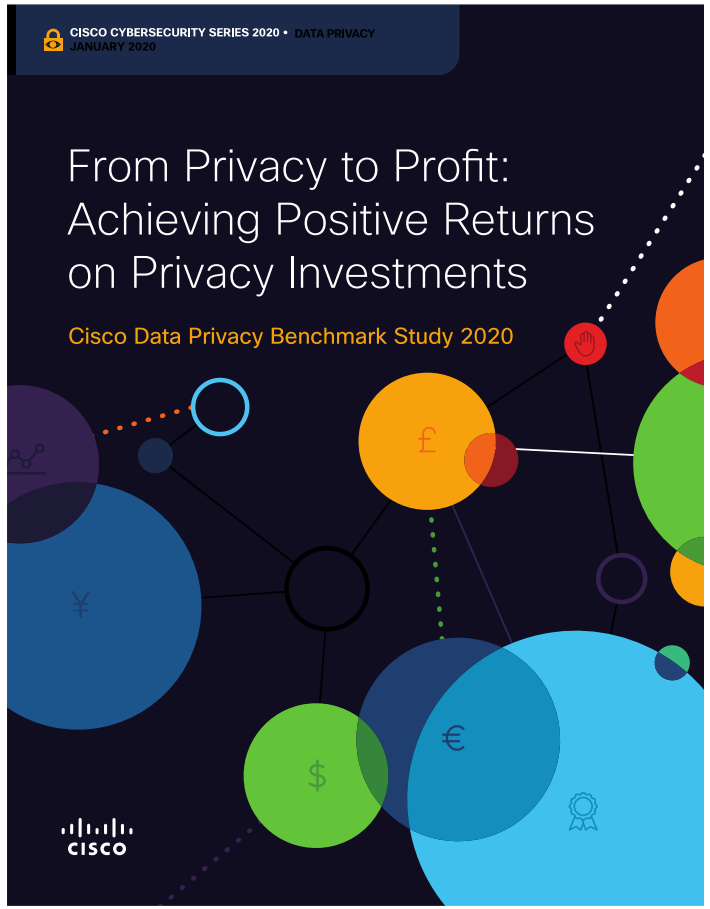
Are able to demonstrate the existence and effectiveness of DPMPs internally (e.g. to the board and senior management) **and externally** (e.g. to privacy enforcement authorities, individuals, business partners and shareholders)

Novas Tendências para Accountability

- Organisations view privacy and accountability as a **digital corporate responsibility and a business enabler**
- **Increasing demands** for accountability from investors and shareholders
- Accountability and global interoperability is **top priority for the Global Privacy Assembly**
- However, **DPAs still question** the effectiveness of accountability for data protection
- **CIPL's accountability mapping project** illustrates common accountability practices
- Regulators can support organisations in their accountability efforts through **guidance and promoting and incentivizing accountability** (e.g. the ICO Accountability Toolkit)
- Now more than ever, accountability is needed in the context of the **COVID-19 crisis**

Cisco's Data Privacy Benchmark Study

Return of Investments on Privacy



Available at trust.cisco.com

Most organisations are seeing **very positive returns** on their privacy investments

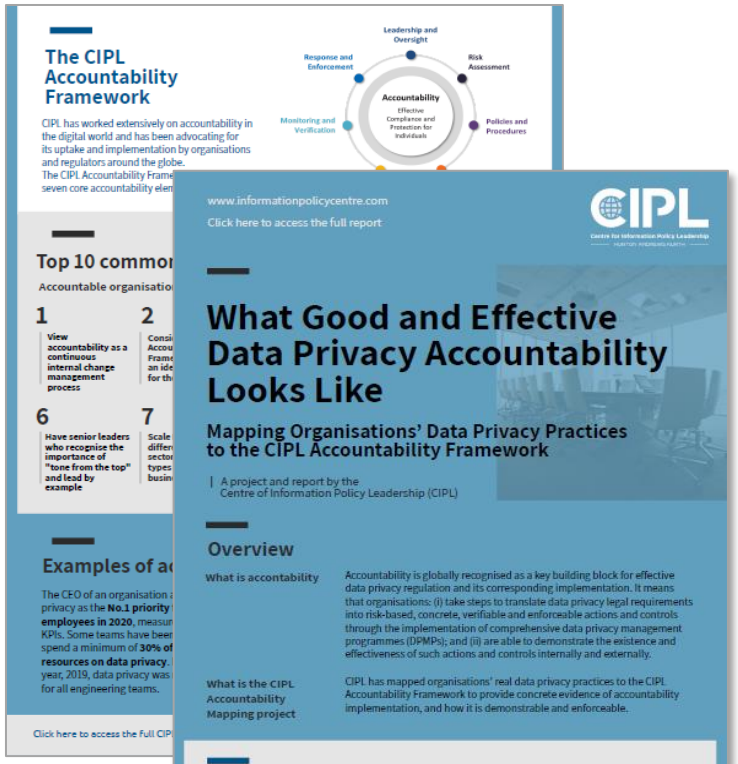
Over 70% are reporting significant privacy benefits in areas such as operational efficiency, agility and innovation

Organisations that are **more accountable** were more likely to have avoided significant breaches, had less downtime, shorter sales delays, and higher returns overall

The vast majority believe **privacy certifications** are important factors in the buying process today

CIPL Accountability Mapping Project

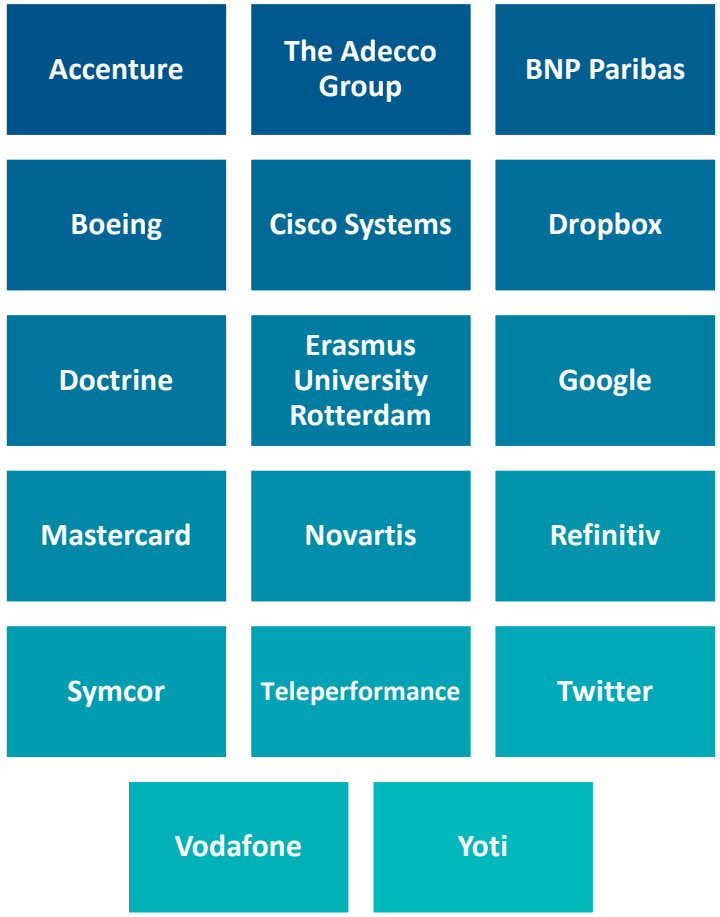
Objetivos do Projeto



- Promote accountability as **standard market practice** and a widely recognised due diligence referential in the digital world;
- Build **global consensus** on accountability between industry and regulators;
- Promote accountability as a **country and sector agnostic framework** and as a bridge between different legal regimes;
- Demonstrate that accountability is a **scalable framework** that works for both big and small organizations;
- Provide **concrete evidence and success stories** from organizations that accountability is demonstrable and enforceable; and
- Promote accountability as a **board-level and a business strategy issue** beyond just legal compliance.

CIPL Accountability Mapping Project

The CIPL Accountability Mapping Report



17 organizações participantes

- Representando variados setores, regiões e tamanhos

Oito meses de trabalho

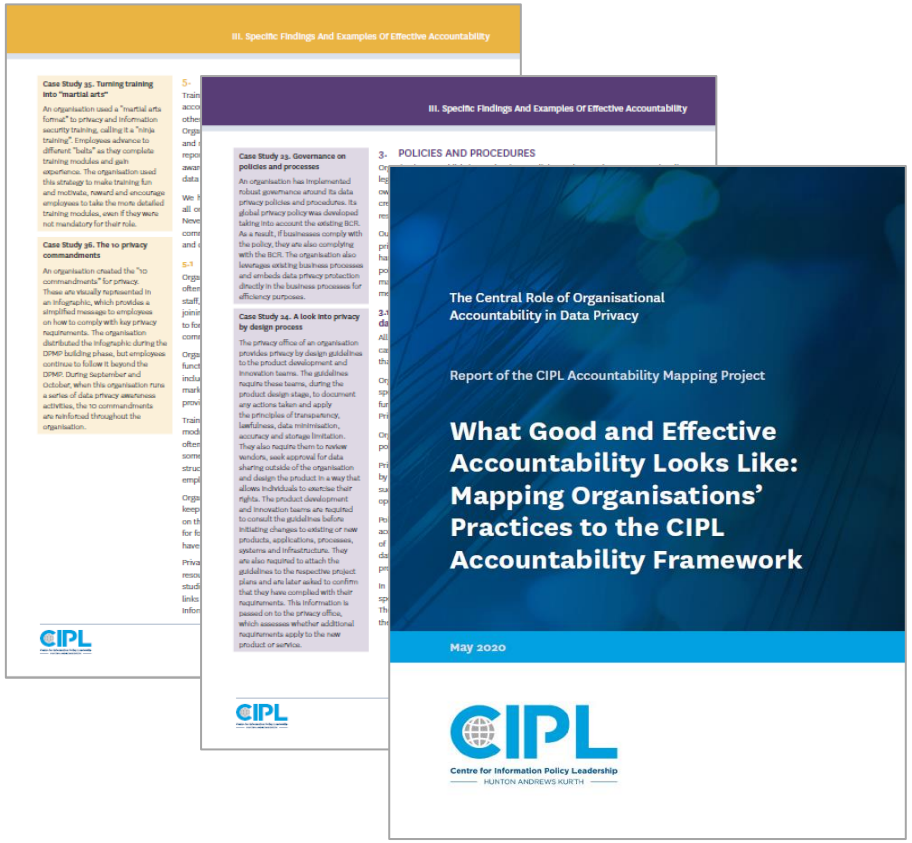
- Entrevistas com Chief Privacy Officers e Data Protection Officers
- Revisão de documentos enviados pelas empresas
- Redação do relatório

46 estudos de caso

- Coletados para demonstrar boas práticas reais de como organizações consideradas accountable implementam os sete elementos do CIPL Accountability Framework

Estrutura do Relatório do CIPL

1. Metodologia e objetivos
2. Top 10 tendências de accountability em proteção de dados
3. Mapeamento de práticas de proteção de dados ao CIPL Accountability Framework e estudos de caso
4. O trabalho do CIPL com accountability organizacional
5. One pager: práticas de privacidade e o CIPL Accountability Framework



Download: https://bit.ly/2Aictev

Top 10 Tendências de Accountability

Conclusões gerais do relatório do CIPL

Accountable organisations:

1 View accountability as a continuous internal change management process

2 Consider the CIPL Accountability Framework as an ideal baseline for their DPMP

3 Recognise accountability as a business topic and enabler of innovation and sustainability

4 Realise business benefits and efficiencies from accountability

5 Embrace accountability both as a controller and as a processor

6 Have senior leaders who recognise the importance of "tone from the top" and lead by example

7 Scale DPMPs to different sectors and types of business

8 Proactively manage data privacy risks and adopt a risk-based approach to their DPMP

9 Are familiar with accountability frameworks as they use similar frameworks in other compliance areas

10 Are driving global convergence in data privacy laws and best practices through a single DPMP

Mapeamento de Práticas de Proteção de Dados

Liderança e Supervisão

DEFINING THE ORGANISATION'S AMBITION, COMMITMENT AND GOVERNANCE | TONE FROM THE TOP | ESTABLISHING A DMPM AND REPORTING

Case Study: Data Privacy made No.1 corporate priority (excerpt from the report)

The CEO of an organisation added data privacy as the No.1 priority for all its employees in 2020, measured by specific KPIs. Some teams have been directed to spend a minimum of 30% of their annual resources on data privacy. In the previous year, 2019, data privacy was made a priority for all engineering teams.

Mapeamento de Práticas de Proteção de Dados

Avaliação de Risco

ASSESSING RISKS TO INDIVIDUALS OF PROJECTS, PRODUCTS AND SERVICES | CALIBRATING THE PRIVACY PROGRAMME AND DATA USES ACCORDINGLY

Case Study: Awareness has driven a volume increase of PIAs and DPIAs (excerpt from the report)

In 2019, a multinational organisation saw a 40% increase on PIAs and DPIAs completed. The organisation undertook over 4,000 assessments. The organisation acknowledged that this was due to the increased privacy awareness within the organisation post-GDPR. Privacy officers were required to prioritise their activities on a daily basis in order to manage the increased workload.

Mapeamento de Práticas de Proteção de Dados

Políticas e Procedimentos

OPERATIONALISING LEGAL REQUIREMENTS AND PRINCIPLES | CONCRETE PROCESSES, ACTIONS AND CONTROLS | ASSIGNMENT OF RESPONSIBILITIES

Case Study: Data privacy and protections flow through the ecosystem (excerpt from the report)

A business-to-consumer organisation believes that protecting individual's data privacy cannot be done in a silo. This is part of a large ecosystem that also includes vendors, partners and third parties who process personal data. The organisation ensures that they are also held accountable, such as through contractual requirements, monitoring of their performance and ultimately terminating relationships.

Mapeamento de Práticas de Proteção de Dados

Transparência

ENHANCING TRUST AND CREDIBILITY INTERNALLY AND EXTERNALLY | TRANSPARENCY TO INDIVIDUALS, PARTNERS, INVESTORS, CLIENTS, REGULATORS

Case Study: Product reviews by customers (excerpt from the report)

A business-to-business organisation allows top-tier customers to review and evaluate the products, even at the source code level, to validate the technical security posture. This allows customers to “trust, but verify” and helps to build and maintain trust in the relationship.

Mapeamento de Práticas de Proteção de Dados

Treinamento e Conscientização

BUILDING A PRIVACY CULTURE INTERNALLY AND CHANGING BEHAVIOURS ON THE GROUND | INNOVATIVE TRANSPARENCY

Case Study: Turning training into “martial arts” (excerpt from the report)

An organisation used a “martial arts format” to privacy and information security training, calling it a “ninja training”. Employees advance to different “belts” as they complete training modules and gain experience. The organisation used this strategy to make training fun and motivate, reward and encourage employees to take the more detailed training modules, even if they were not mandatory for their role.

Mapeamento de Práticas de Proteção de Dados

Monitoramento e Verificação

CLOSING THE ACCOUNTABILITY LOOP | AUDITING AND MONITORING TO TEST COMPLIANCE | OBTAINING PRIVACY CERTIFICATIONS

Case Study: Privacy team monitoring through KPIs (excerpt from the report)

The privacy team of an organisation monitors compliance with privacy controls on a quarterly basis, through reports by local DPOs that include KPIs. All teams involved work intensively to have these ready every quarter. They also get buy-in and understanding from all stakeholders of the importance of this activity, and that this is everyone's responsibility.

Mapeamento de Práticas de Proteção de Dados

Resposta e Execução

ACTING UPON INTERNAL NON-COMPLIANCE | ADDRESSING ENQUIRIES FROM INDIVIDUALS AND REGULATORS | NOTIFYING DATA BREACHES

Case Study: Data access requests process tested by client doing "mystery shopping" (excerpt from the report)

A client decided to test an organisation's process to handle data access requests. The client did a "mystery shopping" — they made an access request without mentioning that they were a client. They were surprised with how promptly and proactively the organisation responded to the request. This led to increased sales with this same client, and therefore generated additional revenues to the organisation.

Obrigada

Giovanna Carloni
Global Privacy Policy Manager
GCarloni@HuntonAK.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton Andrews Kurth Privacy and Information Security Law Blog
www.huntonprivacyblog.com

@THE_CIPL linkedin.com/company/centre-for-information-policy-leadership

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Anexo

CIPL Accountability Papers

Paper Title	Publication Date	Link
Accountability Mapping Report	May 2020	https://bit.ly/2Aictev
Organizational Accountability - Past, Present and Future	30 October 2019	https://bit.ly/2REMkeO
Organizational Accountability in Light of FTC Consent Orders	13 November 2019	https://bit.ly/2GeDZt2
CIPL Q&A on Accountability	3 July 2019	https://bit.ly/33JedYb
Accountability's existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law	3 July 2019	https://bit.ly/2H93vAH
Introduction: The Central Role of Organizational Accountability in Data Protection	23 July 2018	https://bit.ly/2sWkkqQ
The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society	23 July 2018	https://bit.ly/2BaQOSY
Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability	23 July 2018	https://bit.ly/2GbGPjx

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Illustrating Accountability

Examples of accountability practices and content of Data Privacy Management Programmes (DPMPs)

Leadership and Oversight

- Tone from the top and leading by example
- Tone from the middle – management and local level
- Privacy officers, team and local support
- Investing in data privacy talent
- Reporting lines and tools
- Establishing DPMPs and governance
- Internal/External Oversight Boards and Committees

Risk Assessment

- Defining and registering data privacy risks
- Understanding risks to individuals
- Integrating data privacy within risk management
- Managing data privacy risks:
  - at DPMP level
  - at product, service and project levels
  - of business partners and third parties
- Undertaking PIAs and DPIAs

Policies and Procedures

- Internal rules operationalizing data privacy requirements
- Legal basis and fair processing
- Data privacy by design
- Information security and data breaches
- Third party management
- Data transfers mechanisms
- Data maps and records of processing activities
- Other rules (e.g. marketing, HR, M&A)

Transparency

- Transparency to individuals – privacy notices and innovative channels and tools (e.g. privacy portals, user experience and user-centric design, customer journey, dashboards, videos, icons, illustrations, animations)
- Transparency to third parties
- Transparency to regulators

Training and Awareness

- Mandatory corporate training
- Ad hoc and functional training
- Awareness-raising campaigns and communication strategies (e.g. senior leadership videos, data privacy-dedicated dates and events, regular communications, data privacy distributions lists, DPMP branding, quizzes and competitions)

Monitoring and Verification

- Internal and external audits and reviews
- Monitoring, testing, measuring and reporting on effectiveness of the DPMP and on data privacy compliance activities
- Corporate data privacy certifications
- Documentation and evidence (consent, legal bases, privacy notices, PIAs and DPIAs, processing agreements, breach response)

Response and Enforcement

- Acting upon findings of audits and reviews
- Managing individual rights requests and complaints-handling
- Data breach internal reporting and external notification
- Internal enforcement of non-compliance subject to local laws
- Engagement and cooperation with DPAs and other regulators

Organizations must be able to **demonstrate the implementation of DPMPs** – internally and externally

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Accountability in the LGPD

Leadership and Oversight	• Data protection officer • Mandatory LGPD governance program integrated into the organization's general governance structure	
Risk Assessment	• Impact assessment report as requested by the ANPD • Risk assessment of data incidents	• Risk-based approach to development of codes of conduct • Systemic assessment of impact on, and risk to, privacy as part of LGPD governance program
Policies and Procedures	• Legal bases and fair processing • Anonymization procedures • Retention and deletion • Review of automated decisions • Data transfer mechanisms • Internal technical and organisational measures to comply with LGPD	• Security measures for processors • Further technical measures required by the ANPD • Privacy by design • Vendor/processor contracts • Procedures for response to individual rights • Codes of conduct
Transparency	• Access to information about data processing • Special measures for transparency when processing is based on legitimate interests • Special notices for children and elderly	• Goal of the LGPD governance program of building a trust relationship with individuals though transparency and participation mechanisms • Publication of codes of conduct
Training and Awareness	• Ability to demonstrate commitment to adopt internal procedures and policies resulting from the LGPD governance program – training implied	
Monitoring and Verification	• Evidencing consent • Verifying parental consent • Legitimate interest impact assessment • Internal records of processing	• Internal and external compliance monitoring for the LGPD governance program • Assessment of effectiveness of the LGPD governance program
Response and Enforcement	• Data incident response plans and remediation, breach notification • Audit for discrimination resulting from automated decision-making • Processor liability	• Demonstrating effectiveness of the LGPD governance program • Sanctions for non-compliance • Mandatory public consultation for ANPD guidance and requirements • Public hearings organised by the National Council