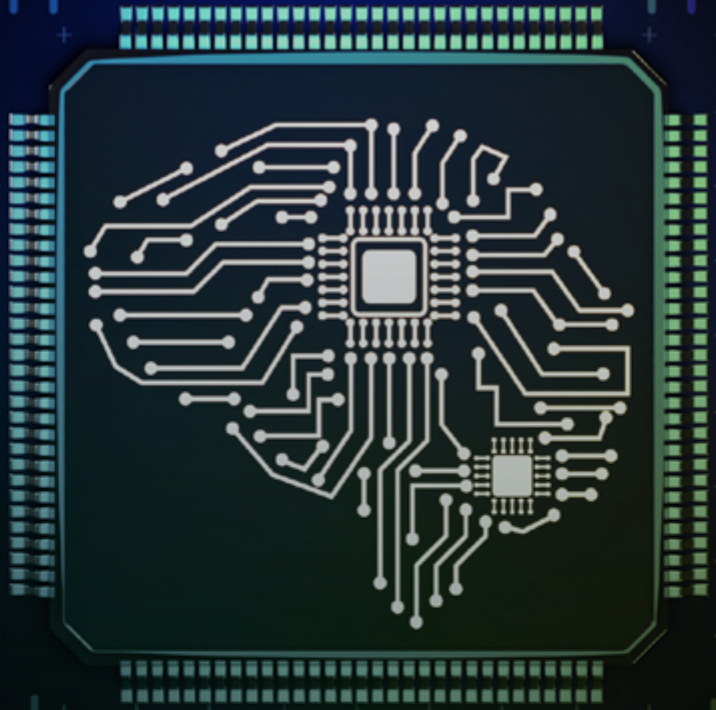
ADV

Where Law
Drives Innovation



eBook

THE ROLE OF THE DPO IN AI GOVERNANCE

Real Challenges, Key Functions, and Practical Solutions

MAIN TOPICS:

- Distinction between the roles of DPO and CAIO;
- Convergence between data governance and AI;
- Practical comparison between GDPR and AIA;
- New challenges regarding the rights of data subjects and individuals affected by automated systems;
- **Over 60 practical criteria in checklist format.**

www.vlklaw.com.br

August, 2025

INDEX

Contextualization

Artificial Intelligence ("AI") is a transformative general-purpose technology that is redefining how companies operate, becoming increasingly ubiquitous across activities and sectors.

On the other hand, there are profound challenges, such as: abrupt transformations in the labor market; challenges related to explainability, auditability, supervision, and control of automated decisions using AI; preservation of copyright in training large-scale models; cybersecurity; privacy; unfair algorithmic discrimination; deepfakes and manipulations; dependency and excessive trust; and the concentration of power in a few countries and companies.

These issues, combined with the intense processing of personal data in AI applications, **have required a strategic review of traditional governance practices** and the effective integration of technical, legal, and ethical requirements. **At the center of this convergence lies the role of the Data Protection Officer** (hereafter referred to as "DPO").

The function of the DPO, traditionally linked to regulatory compliance in personal data protection, **tends to expand in light of the impacts of AI, requiring an even more strategic, cross-functional, and multidisciplinary role.**

The complexity intensifies when considering the international context. Various jurisdictions impose distinct regulatory obligations, such as: the General Data Protection Regulation ("GDPR") in the European Union; the Lei Geral de Proteção de Dados Pessoais ("LGPD") in Brazil and its regulation; and emerging AI regulations, such as the EU AI Act, Bill 2338/2023, the international standard ISO/IEC 42001:2023, the AI Risk Management Framework from NIST, and the OECD AI Principles.

The AI Index Report 2025, developed by Stanford University (USA), focusing on governance, compliance, and strategic AI risks in companies, **identifies privacy and personal data protection as the risk that most concerns companies in terms of AI (65%)**, followed by technical reliability in the face of inaccuracy and hallucination (59%), intellectual property (56%), and financial losses (59%)[1].

In this scenario, **the DPO must work even more in coordination with business leaders**, those responsible for innovation, technology, and digital transformation, and new roles such **as the Chief Artificial Intelligence Officer ("CAIO")**, to ensure legal compliance, stakeholder trust, and organizational accountability regarding algorithmic risks, with or without the use of AI. This is a challenge that extends beyond traditional compliance, involving institutional governance, digital maturity, and an organizational culture guided by ethics, explainability, transparency, and non-discrimination.

This eBook was developed to **support DPOs in the practical, comparative, and strategic understanding of this new intersection between data protection and AI governance.** We will explore:

- The distinctions and synergies between the roles of DPO and CAIO;
- The points of convergence between data and AI governance structures;
- The technical and methodological comparison between the Data Protection Impact Assessment ("DPIA") and the Algorithmic Impact Assessment ("AIA"); and
- The legal and practical challenges related to the rights of data subjects and individuals affected by automated systems.

Each chapter is accompanied by a practical and structured checklist, with over 60 evaluation criteria. The goal is to provide functional tools applicable to the reality of organizations, reinforcing this material's commitment to technical content that is direct and effectively useful for those working on the front lines of data protection, considering the new challenges brought by algorithmic transformation.

VLK Advogados

1. DPO and CAIO: Distinctions, Role Overlaps, and Practical Challenges

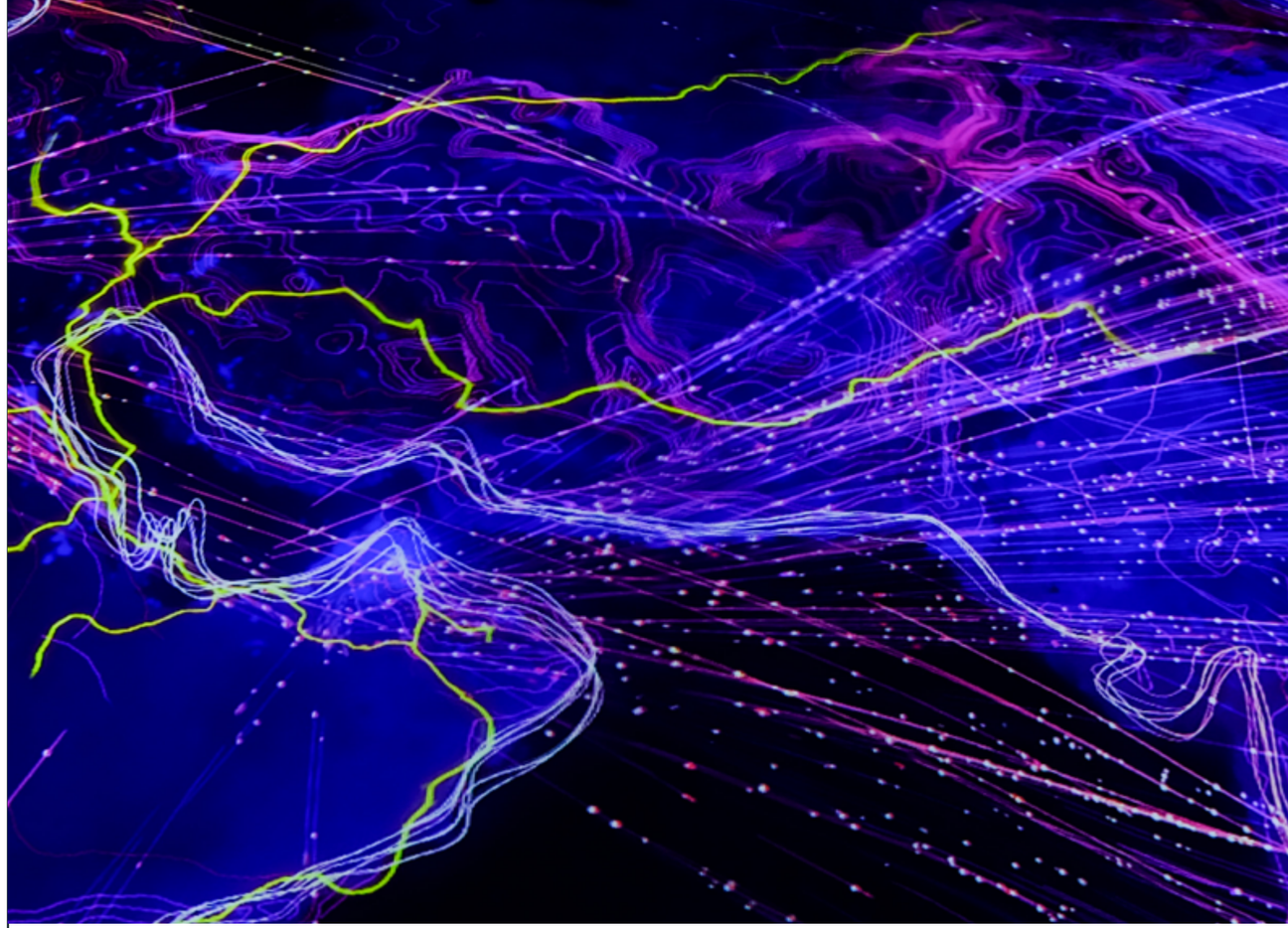
The consolidation of AI as a general-purpose, ubiquitous, and strategic technology within organizations has prompted a reorganization of roles and responsibilities in digital governance. In this new scenario, figures such as the CAIO emerge, whose role must be clearly defined, **including mitigating the risk of conflicts of interest and overlaps with the DPO's responsibilities.**

While the DPO's central role is to ensure compliance with data protection regulations and mitigate risks, enabling the development of new business models that respect the principle of Privacy by Design ("PbD"), **the newly established CAIO position aims to drive AI adoption and orchestrate the cultural shift necessary for the technology to be integrated throughout the organization,** typically with the following responsibilities:

- *D*efine the organization's AI strategy;
- Drive cultural change and develop competencies;
- Act as a bridge between technology and business;
- Conduct statistical analyses, machine learning algorithm assessments, and data infrastructure evaluations for effective AI solution implementation;
- Address ethical and legal AI issues, such as undue bias, accountability across the AI value chain, robustness, safety, and transparency.

Although Chief Technology Officers (CTOs) and Chief Innovation Officers (CIOs) currently lead most digital transformation initiatives within companies, recent global research[2] reveals that companies are appointing a dedicated AI executive—the CAIO—to accelerate adoption and manage implementation complexity:

- In Brazil: 56% of organizations already have a CAIO, and another 31% plan to appoint one by 2026;



- *Globally: the current figure is 60%, with projections to reach 86% by 2026.*

Other relevant figures from Brazil: only 28% of Brazilian companies have a structured strategy to integrate AI into business processes. However, 93% recognize the importance of effective management to incorporate the technology into their operations. It is forecasted that by the end of 2026, 91% of companies will have dedicated strategies to manage the impact of AI.

In the U.S., the new AI strategy, "AI Action Plan USA"[3], addresses the Chief Artificial Intelligence Officer Council (CAIOC) in the context of accelerating AI adoption within government, recommending the formalization of the position as the primary body for interagency coordination and collaboration in AI adoption, in strategic alignment with other relevant federal executive councils, including: the President's Management Council, Chief Data Officer Council, Chief Information Officer Council, Interagency Council on Statistical Policy, Chief Human Capital Officer Council, and the Federal Privacy Council.

A Gartner survey[4] shows that **AI responsibilities are dispersed,** as follows:

- *Of the 54% of executives who reported having an AI leader, 88% said this lea*der did not hold the CAIO title;
- For 25% of companies, AI responsibility lies with the CIO;
- 55% of organizations have a multidisciplinary AI council to address the challenge of delivering value and reducing risks;
- W*ithin the council, the main areas of focus are: 26% governance and 21% strategy for addressing AI.*

In the United Kingdom, nearly half (48%) of companies in the Financial Times Stock Exchange (FTSE) 100 have already established AI leadership roles, with three predominant areas of focus: data science (50%), consulting (21%), and engineering and technology (17%)[5].

In terms of AI governance, the AI Governance Profession Report 2025[6], involving more than 670 companies in 45 countries, indicated that:

- 77% of companies are adopting AI governance;
- Over 50% of AI governance professionals typically come from ethics, compliance, privacy, or legal teams;
- Primary functions responsible for AI governance: 25% privacy, 22% legal, 17% technology, 10% data governance, 6% ethics and compliance, and 5% cybersecurity;
- When the primary AI governance responsibility lies with the organization's privacy officer, respondents were significantly more likely to feel confident in their ability to comply with the EU AI Act (67%).

Thus, this chapter addresses the limits of role overlaps, the risks of conflict of interest, and possible operational models depending on the organization's size and maturity.

1.1. ROLE CONVERGENCE AND THE EMERGENCE OF NEW POSITIONS

With the rise of AI in business operations, strategic roles focused on algorithmic governance are emerging, particularly given the interdependence between Artificial Intelligence and data protection. While the DPO plays a central role in compliance with the LGPD, the CAIO addresses the increasing complexity of algorithmic systems and the need to ensure ethics, transparency, and accountability in their implementation, regardless of whether personal data is involved. Both have cross-functional roles and share common objectives, such as:

- Preventing regulatory and reputational risks;
- Promoting trust in emerging technologies;
- Ensuring the success of new business strategies and corporate digital transformation, increasingly driven by data and AI algorithms; and
- Safeguarding fundamental rights.

They are, therefore, **complementary roles but with specific and distinct technical competencies.** For this reason, many AI governance programs are supported by mature data protection structures.

Research indicates that **half of organizations structure their AI policies based on existing privacy frameworks**[7], with particular emphasis on DPIAs, which have been adapted to develop AIAs (a topic addressed explicitly in Chapter 3). This reinforces the **DPO's strategic role, especially in risk mitigation, system explainability, and fundamental rights.**

Given this scenario, the question arises: can the roles of DPO and CAIO be held by the same person? To what extent is such a merger of functions feasible?

1.2. OVERLAP: OPPORTUNITY OR TRAP?

Based on our practical experience in structuring and updating data protection and AI governance, we have observed:

- DPOs leading AI governance efforts;
- CAIOs spearheading certain aspects of algorithmic privacy; and
- Data protection and AI governance teams working in an integrated manner but under distinct leadership.

Overlap may lead to gains in agility and cohesion, **provided that limits related to autonomy, impartiality, and specialization are respected,** while also considering the organization's size and the risks associated with AI projects.

The GDPR (Art. 38) and Brazil's CD/ANPD Regulation No. 18/2024 **require technical independence and absence of conflicts of interest for DPOs.** The same professional should not supervise compliance while also making strategic decisions about data processing or AI implementation.

The Belgian Data Protection Authority fined a company that combined the DPO and compliance director roles. Positions such as CIO and CEO are also considered potentially incompatible with the DPO role.

The Court of Justice of the European Union (CJEU) reinforced this view in case C-453/21, affirming that the DPO's independence is compromised when they define the purposes and means of data processing. The conflict-of-interest assessment must consider the organizational structure and internal policies.[8]

In Brazil, the "Guidance on the Role of the DPO" based on CD/ANPD Regulation No. 18/2024, issued by the National Data Protection Authority (ANPD)[9], provides:

> In general, conflicting positions are observed when the DPO holds leadership, management, or executive roles responsible for determining the means and purposes of personal data processing, such as departments responsible for human resources management, **information technology,** finance, or healthcare. (emphasis added)

While the DPO adopts a supervisory and moderating stance[10], the CAIO acts as an AI leader for integrating technology into digital transformation and innovation. This difference in focus may make role overlap complex for governance roles such as the DPO's role.

1.3. MODELS BASED ON ORGANIZATIONAL SIZE, COMPLEXITY, AND MATURITY

The ideal AI governance structure generally considers three factors:

- Organization size;
- Complexity and intensity of AI systems and associated risks; and
- Level of maturity in digital governance.

In small and medium-sized enterprises, combining roles is common, often due to budgetary constraints. In such cases, the DPO may have an expanded role, provided that:

- A formal conflict assessment is conducted;

» Justifications are documented; and

» Safeguards are in place, such as direct reporting to the Board or Senior Management.

In larger companies with complex or high-risk projects, the trend is to separate the roles of DPO and CAIO, each with its own technical scope and decision-making autonomy.

Intermediate roles, such as AI Risk Officer (dedicated to identifying, assessing, and mitigating algorithmic risks), are also gaining ground, focusing on risk mitigation, working alongside the DPO but without executive interference.

To ensure effectiveness, legal certainty, and transparency, the organization must establish:

» Clear definitions of scope and authority for each of these roles;

» Independent reporting protocols; and

» Collaborative workflows between legal, data, technology, and compliance teams.

Structured collaboration between the DPO, CAIO, and other stakeholders is essential for AI systems to be technically robust, legally compliant, and socially trustworthy.

1.4. CHECKLIST FOR THE DPO

a) Independence and Conflict of Interest

☐ My current responsibilities do not include operational decisions about AI (models, criteria, or implementation).

☐ There is a formal and documented assessment of the absence of conflict of interest, as required by the ANPD.

☐ If I hold other roles, they do not affect my impartiality as a DPO.

☐ I have technical autonomy to issue opinions contrary to the AI strategy, if necessary.

b) Structure and Reporting

☐ My role is formally documented, with clear scope and responsibilities.

☐ I report directly to Senior Management or the Board.

☐ I participate in risk committees but do not hold executive responsibility over AI.

c) Collaboration with the CAIO and other stakeholders

☐ There are structured collaboration processes with the CAIO and technical teams.

☐ AI governance includes fundamental rights, privacy, and explainability.

☐ I participate in Algorithmic Impact Assessments (AIAs) that involve personal data or data subject rights.

d) Model proportional to organizational size and maturity

☐ The current structure (combined or separate roles) was adopted based on a formal analysis of the organization's size, budget, risks, and digital maturity.

☐ In cases of role combination, safeguards such as independent reporting, external validation, or periodic review were implemented.

☐ I have established a mechanism to review the organizational structure as risks and projects evolve.

e) Continuous Training and Updates

☐ I receive ongoing training on AI, algorithmic risks, and regulations (AI Act, LGPD, GDPR, ISO 42001, among others).

☐ I monitor regulatory decisions and best practices regarding the DPO role and its interface with AI governance.

2. Data Protection Governance and AI Governance: Leveraging Frameworks, Resources, and Policies

As AI consolidates itself as a strategic asset, there is growing demand for governance models capable of integrating privacy, ethics, security, and algorithmic accountability. The challenge lies in leveraging well-established data protection frameworks and structuring AI governance with budgetary and technical efficiency.

The Brazilian National Data Protection Authority (ANPD), in its analysis of AI Bill No. 2.338/2023[11], aligns with this understanding:

> The LGPD introduced the concept of data governance in Brazil, establishing the need for organizations to implement robust policies, practices, and procedures to ensure personal data protection. Bill No. 2.338/2023, in addressing AI regulation, also emphasizes the importance of strong governance mechanisms for AI systems, especially those classified as high risk. **The experience and guidelines already established by the LGPD can serve as the basis for the development of specific governance mechanisms for AI.** (emphasis added)

But what are the main challenges in governing AI? The previously mentioned AI Governance Profession Report 2025 points out:

- 49% – lack of understanding about AI and compliance obligations related to the technology;
- 37% – insufficient resources dedicated to AI governance activities;
- 35% – lack of representation of the AI governance function at senior levels of the organization;
- 31% – competing priorities that reduce focus on AI governance activities;
- 27% – ineffective integration of AI risk management with broader organizational risk management activities; and
- 26% – Privacy by Design is not effectively implemented within the organization.

The same report highlights interesting case studies from certain companies regarding the integration between AI governance and data protection[12], such as:

- **Mastercard:** when an AI risk is considered potentially high, it is reviewed by the AI and Data Council, composed of senior leaders from various areas and co-chaired by the Chief Privacy Officer and the Chief AI and Data Officer;
- **IBM:** the “Chief Privacy Office” (later renamed the “Office of Privacy and Responsible Technology”) was tasked with ensuring responsible AI development and deployment. This department expanded the original program developed to identify privacy impact assessments and GDPR

compliance to incorporate AI and general data governance.

- **Randstad:** AI governance is operated from the legal and data protection department.

- **TELUS:** the company had a history of developing technologies that required considerations of data ethics, governance, and privacy. This enabled existing teams to address AI governance challenges quickly.

Thus, this chapter explores this practical and conceptual convergence, identifying pathways, limitations, and best practices.

2.1 EVOLVING STRUCTURES AND POINTS OF CONVERGENCE

Digital governance is fostering the integration of data protection and AI. Both share areas of concern, such as:

- Risk prevention and information security;

- Guaranteeing rights; and

- Transparency and accountability.

Established frameworks (such as DPIAs, Privacy by Design policies, and data governance committees) are often the starting point for AI governance. They allow the inclusion of:

- Algorithmic Impact Assessment (AIA);

- Fundamental Rights Impact Assessment (FRIA)[13];

- Inventory (or mapping) of AI systems;

- Training programs and organizational culture (e.g., "AI Champions"); and

- Adapted policies and contracts (with specific clauses).

International standards, such as the NIST AI RMF (2023), EU AI Act, ISO/IEC 42001, OECD AI Principles, and guidelines from the European Data Protection Board

(EDPB) and the ANPD[14] reinforce the centrality of data protection principles as the basis for responsible AI, including:

- Risk-based approach;

- Governance mechanisms; and

- Incident reporting.

2.2 STRATEGIC COMMUNICATION: A COMMON PILLAR

Active transparency is an essential component of both structures, including for: data subjects and affected individuals; regulators; and the general public. These governance structures must:

- Use accessible language and legal design in communications;

- Structure clear channels for complaints and responses; and

- Promote institutional trust, especially in critical sectors (finance, health, insurance, education, telecommunications, energy, and public safety).

The reuse of response channels and structures already in place for data protection in the AI context is therefore an efficient and sustainable practice.

2.3 REUSE OF STRUCTURES AND TOOLS

We highlight examples of data governance structures that can be extended

or adapted to AI governance, based on the conducted inventory and the risks identified for mitigation:

Tool/Structure	Use in Privacy	Adaptation for AI
Governance Program	Policies, indicators, and action plans	Inclusion of ethical pillars and algorithmic risk and performance metrics
DPIA	Risk assessment and mitigation measures	Basis for AIA and FRIA, with expanded scope
Privacy Committee	Risk deliberation and data decisions	Expansion to the AI and Ethics Committee
LGPD Training	Privacy training	Inclusion of specific concepts and topics like bias, explainability, and ethics
Codes and Policies	Internal rules on data processing	Extension to responsible, ethical, explainable, and auditable AI use
Data Subject Rights Management	Responding to access, deletion, correction, etc.	Expansion to automated decisions, human review, and AI explainability
Transparency and Purpose Principles	Privacy notices and clear communication of purposes	Inclusion of transparency about the algorithmic criteria and the AI usage purpose
Third-Party Contract Clauses	Data protection obligations with suppliers	Insertion of specific requirements on AI use, risk assessment, and technical audits
Third-Party Risk Assessment	*Operator due diligence*	Audit of algorithmic practices and ethical/ regulatory alignment of AI providers
Incident Reporting	Evaluation of security incidents with risk/ damage	Evaluation of serious incidents involving threats to life, critical systems, or fundamental and environmental rights violations

Source: VLK Advogados

2.4 SUSTAINABILITY AND ORGANIZATIONAL MATURITY

According to the IAPP-EY Privacy Governance Report 2023[15] and Cisco Privacy Benchmark, companies with mature privacy programs are better prepared to structure AI policies. This includes: dedicated budgets (average of US$2.7 million in 2023); specialized teams; and consolidated ESG strategies.

The main obstacle, however, is the lack of training: 51% of companies identify the absence of internal knowledge as a barrier to responsible AI. The DPO must be involved from the conception of AI projects involving personal data, offering critical insight and guiding decisions based on legal and ethical principles[16]. Integrating both governance frameworks promotes:

- Reduction of regulatory costs through shared structures;
- Clarity of roles and responsibilities; and
- Strengthening of an organizational culture oriented toward ethics and innovation.

AI governance is not an isolated task, but a living structure, tailored to risks, stakeholders, and technological maturity. The DPO's role is to be one of the pillars of this structure, working in synergy with other leaders to ensure AI use is innovative, effective, and responsible.

2.5 CHECKLIST FOR THE DPO

a) Integrated Governance Structure

- ☐ The organization has an institutional program that integrates personal data and AI.
- ☐ There is a multidisciplinary committee for ethics, risk, and AI decisions, with a structured and approved regulation.
- ☐ DPIAs are used as a basis for preparing AIAs.
- ☐ Data governance policies include specific guidelines for automated systems.

b) Strategic Communication and Transparency

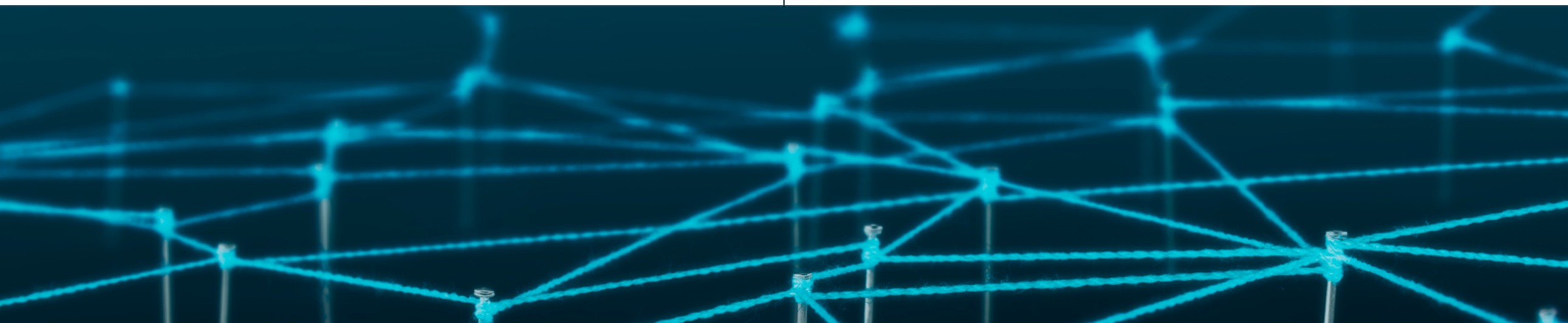
- ☐ Communications explain AI use and automated criteria in clear, accessible language.
- ☐ Privacy notices include specific mentions of AI's purpose.
- ☐ Response channels are prepared for AI-related requests.
- ☐ Legal design is used in public-facing materials to promote genuine understanding of algorithm use.

c) Reuse of Structures and Tools

- ☐ The privacy committee also addresses ethics and AI risk.
- ☐ Training includes topics such as bias, explainability, algorithmic accountability, and ethical AI use.
- ☐ Contracts with third parties include clauses on AI, audits, and risk mitigation.
- ☐ The organization conducts technical and ethical due diligence on third parties that develop or operate AI solutions.

d) Sustainability and Organizational Maturity

- ☐ The AI structure reuses processes and resources from data governance.
- ☐ There is a dedicated or shared team and budget for responsible AI initiatives.
- ☐ The DPO is involved from the start of AI projects involving personal data, contributing to risk assessment and defining ethical and legal safeguards.
- ☐ The adopted model respects the stage of digital maturity and is reviewed as projects and risks evolve.



3. DPIA and AIA: Practical Comparative Analysis

Responsible AI governance requires prior assessment of the risks and impacts that these technologies may generate. In this context, the DPIA and AIA are central tools, often confused or applied in isolation. This chapter provides a technical, legal, and strategic analysis of these two mechanisms, highlighting their differences, points of complementarity, and pathways toward an integrated structure.

3.1 FUNDAMENTAL CONCEPTS: PURPOSE AND SCOPE

The DPIA is required by the LGPD (Articles 5, XVII, and 38) and by the GDPR (Article 35) in situations where the processing of personal data poses a high risk to the rights and freedoms of data subjects. Its purpose is to map data processing operations, identify legal bases, assess and mitigate risks related to the use of personal data, and propose mitigation measures.

The AIA, in turn, has a broader scope, going beyond personal data protection and analyzing the technical and ethical operation of the AI system, addressing topics such as:

- Algorithmic opacity;
- Bias;
- Violation of third-party rights;
- Environmental impacts;
- Algorithm unpredictability, possible negative externalities, and loss of autonomy.

Although not legally mandatory in many contexts, its voluntary adoption is recommended to mitigate reputational and regulatory risks.

Indeed, the AIA is provided for in Bill No. 2.338/2023[17] as an obligation of the developer or deployer who introduces or places an AI system on the market whenever the system or its use is deemed high risk, considering the role and participation of the agent in the chain.

The EU AI Act, although it does not use the term "AIA" broadly to refer to a single impact assessment, provides (Article 27), among other risk management forms, the Fundamental Rights Impact Assessment (FRIA), required from entities implementing high-risk AI systems and that are public bodies or private operators delivering public services, or operators implementing credit scoring systems (except fraud detection) or systems used for risk assessment and pricing in life and health insurance. The evaluation must detail the intended use of the system, identify the affected populations, and assess potential risks to fundamental rights. The results must be reported to the competent authority.

3.2 TECHNICAL AND METHODOLOGICAL COMPARISON

Despite their differences, DPIA and AIA share methodological foundations: risk identification, mitigation measures, and structured documentation. Below are some practical comparative points:

Item	DPIA	AIA and FRIA
Normative Basis	LGPD and GDPR	EU AI Act, NIST AI RMF, OECD AI Principles, ISO/IEC 42001
Trigger for Application	Processing of personal data involving high-risk, sensitive data, or based on legitimate interest	Development, acquisition, or use of AI systems, especially high-risk
Main Focus	Privacy, data protection, legal compliance	Technical, ethical, and social risks related to AI use
Subject of Analysis	Personal data and processing operations	The AI system as a whole: model, logic, data, usage context
Lifecycle Analyzed	Entire lifecycle: collection, use, storage, sharing, and deletion	Entire AI system lifecycle: design, testing, deployment, and monitoring
Multidisciplinary Involvement	Legal, DPO, information security	Legal, DPO, engineering, data science, compliance, ethics
Risk Aspects Covered	Legal basis, minimization, security, and data subject rights	Bias, explainability, accuracy, robustness, social and discriminatory impacts

Source: VLK Advogados

3.3 COMPLEMENTARITY AND REUSE

The integration between DPIA and AIA is both possible and advisable, especially when the AI system involves the processing of personal data. The DPIA can serve as the legal-regulatory foundation for constructing the AIA, which will broaden the scope of analysis and incorporate technical-social aspects of algorithmic governance, including:

- Assessment of discriminatory bias and unequal impacts on social groups;
- Verification of explainability, robustness, and accuracy of automated systems;
- Analysis of externalities, collective risks, and systemic effects on fundamental rights.

Both the EU AI Act and Bill 2.338/2021 foresee the reuse of existing DPIAs as a foundation for the AIA, provided that the content is expanded[18] to include technical and ethical aspects specific to AI, bringing:

- The technical functioning of the AI system;
- Ethical and non-personal data-related risks;
- Specific AI measures, such as human oversight and bias mitigation;
- Statistical accuracy, technical robustness, and protection against

adversarial attacks; and

» Explainability and environmental impact.

The ANPD has also expressed this view[19]:

> Both mechanisms comprise governance tools aimed at anticipating and addressing potential problems before they occur. For effective governance, it is essential to have clarity on how these two mechanisms relate and complement each other. The relationship between these assessments may be considered, ensuring that, when evaluating AI systems, both algorithmic and data protection impacts are addressed in an integrated manner.

In practice, the DPO may lead the preparation of the DPIA and collaborate on or even develop the AIA, respecting the technical limits of their role. In mature organizations, this integration enables a more holistic risk view and ensures legal compliance along with ethical responsibility and technical security.

3.4 LIMITATIONS AND PRAGMATIC ACTIONS

When applied in isolation, DPIA and AIA may leave gaps in analysis, undermining governance effectiveness. See examples:

Critical Situation	Associated Risks	Recommended Actions
Conducting only the DPIA in AI projects	Ignores bias, explainability, and ethical impacts	Expand the DPIA scope to include essential AIA elements
Conducting an AIA without a structured legal analysis	Legal uncertainty about data processing	Integrate legal analysis in line with LGPD, GDPR, and other legal bases
Producing isolated formal documents	Low practical effectiveness and risk of disconnection between departments	Create integrated and functional models

Source: VLK Advogados

3.5. CHECKLIST FOR THE DPO

a) Integrated Application

- ☐ I am clear on when to use the DPIA, the AIA, or both.
- ☐ The documents are integrated or complementary, avoiding rework and scope gaps.
- ☐ In AI projects involving personal data, I always consider LGPD requirements, as well as AI Act, Bill 2.338, and other governance frameworks.

b) Methodology and Participation

- ☐ There is a formal methodology for conducting DPIAs and AIAs, with defined stages, responsibilities, and criteria.
- ☐ The assessments involve multidisciplinary participation: legal, technical, information security, and data science.
- ☐ The analyses include technical (robustness, accuracy), legal (legal basis, rights), and ethical (bias, social impact) aspects.

c) Reuse and Efficiency

- ☐ DPIAs are reused as direct inputs for composing or initiating AIAs.
- ☐ The team is familiar with reference models (NIST AI RMF, OECD AI Principles, ISO/IEC 42001) and applies them as needed.
- ☐ There is an organized history of past assessments, with lessons learned and a monitored action plan.

d) Limitations and Corrective Actions

- ☐ Limitations of each assessment type are mapped, and complementary actions are adopted (e.g., simulations and external reviews).
- ☐ There is a procedure for periodically reviewing DPIA and AIA documents, especially after changes in AI models.
- ☐ The organization can justify, in a documented manner, why an assessment was performed or waived.

4. Rights of Data Subjects and Affected Individuals: Challenges and Paths to Integrated Governance

4.1.TWO REGULATORY FRAMEWORKS, ONE COMMON CORE: THE INDIVIDUAL

Personal data protection (LGPD, GDPR) and AI governance (AI Act, ISO/IEC 42001, NIST AI RMF) are based on different premises but converge on a fundamental point: the protection of the human person.

- The LGPD is structured around data subjects.
- The AI Act and other AI-related norms broaden the focus to include any person affected by algorithmic systems, even if not identifiable in the processed data.

This expansion demands a new regulatory outlook: not all AI risks stem from the use of personal data, but high-risk AI can impact fundamental rights—even of those who are not data subjects in the strict sense of the LGPD.

4.2 IMPLEMENTATION CHALLENGES: AI, BIAS, AND TRANSPARENCY

AI technologies challenge the practical applicability of rights established by data protection laws. Four main challenges are involved:

- **Algorithmic biases** that affect groups or communities;
- **Automated decisions** with significant impact, but no clear identification of the affected "data subject";
- **Difficulty in explainability,** which compromises the exercise of review and objection rights;
- **Derived or inferred data,** not provided by the subject, but directly affecting their life.

The LGPD (Art. 20) guarantees the right to review automated decisions, but its practical effectiveness is still limited. The GDPR goes further by allowing data subjects to request human review. A decision by the Court of Justice of the European Union (CJEU) reinforced this requirement by ruling that the absence of human review in credit scoring systems is unlawful, constituting a violation of informational self-determination[20].

AI governance must be built upon algorithmic fairness, transparency, and proportionality, going beyond the traditional perspective of the "data subject."

It is important to remember that the fundamental right to transparency and to understanding how automated decisions affect individuals does not imply disclosing the algorithm or all its technical complexities, which could compromise trade secrets. What is required is a comprehensible and helpful explanation of the logic behind the decision.

Most automated decisions do not pose high risks. Algorithm explainability must be weighed and applied according to the respective risk to individuals.

Moreover, the heterogeneity of user profiles requires that explainability be treated as a graduated communication process, not as a single, generic, or overly technical response. A recommended practice is the adoption of layered explanations: beginning with an accessible overview of the decision's logic, followed by deeper levels based on the interest, need, and understanding of the audience, while protecting trade secrets.

Explainability models should translate the "logic" of the algorithm into comprehensible terms without disclosing the source code, such as: explaining which factors were considered by the system to reach the decision; identifying which data were most relevant in the prediction; showing how variations in those data affect the outcome; and indicating the possible consequences of the automated decision.

4.3 FROM DATA PROTECTION TO HUMAN PROTECTION

Effective governance requires a focus on the effects of AI on individuals. The DPO, who may also take on AI governance functions, must evolve from a compliance guardian to an orchestrator of ethical, social, and technical protection. This requires coordinated action with risk, technology, compliance, and human rights areas.

It is at this convergence that DPIAs and AIAs gain relevance. Both should

protect not just data, but people. The focus must be on mitigating individual and collective impacts. To this end, it is recommended to:

- Extend the concept of "data subject" to include individuals affected by algorithmic decisions (especially in high-risk assessments);
- Incorporate the concept of "affected person" into impact reports and response channels;
- Assess collective impacts as part of regulatory and reputational risk.

4.4 LEGAL INTERPRETATION AND INTEGRATED GOVERNANCE PATHS

To mitigate risks, anticipate possible regulatory requirements, and build trust among data subjects and affected individuals, it is advisable to:

- Expand rights-exercise channels to include mechanisms for reviewing, contesting, and clarifying automated decisions;
- Revise privacy policies based on Legal Design and Visual Law, detailing the impacts of AI;
- Integrate the DPO and CAIO into ethics and risk committees, especially in contexts of collective impact; and
- Create active listening mechanisms with stakeholders, including user testing and continuous feedback.

4.5 CHECKLIST FOR THE DPO

a) Understanding and Scope

- [ ] I acknowledge that not all AI impacts are limited to personal data protection.
- [ ] Policies and reports also consider indirectly affected individuals, even if not data subjects under the LGPD.
- [ ] Impact assessments address social, ethical, and collective risks, in addition to legal ones.

b) Transparency and Communication

- [ ] Communications regarding AI use are clear about decision criteria, logic, and potential effects.
- [ ] There is an option to request human review for demonstrably high-impact automated decisions.
- [ ] Simple language, Legal Design, and educational strategies are used.

c) Exercise of Rights

- [ ] Service channels consider both data subjects and any person affected by AI.
- [ ] Effective mechanisms are in place for reviewing, contesting, and clarifying automated decisions.
- [ ] Data subject rights are adapted to algorithmic realities (explainability, proportionality, and non-discrimination).

d) Collaborative Governance

- [ ] The DPO and CAIO work together on cases with the potential to affect fundamental rights broadly.
- [ ] The governance committee considers impacts on vulnerable groups.
- [ ] There are clear protocols for responding to complaints, adverse effects, or security incidents.

Final Considerations

As algorithmic systems become more sophisticated and socially impactful, the roles of the DPO and CAIO gain strategic relevance. The DPO, once confined to personal data compliance, now plays a cross-functional role in digital governance, identifying risks, assessing ethics, and promoting transparency. The CAIO, on the other hand, emerges as a leader focused on innovation and AI strategy execution, also sharing responsibility for algorithmic integrity.

Throughout this eBook, we have examined the distinction and potential overlap between these two roles. Practical experience and insights from regulatory authorities worldwide indicate that combining functions requires a conflict-of-interest analysis.

We also demonstrated that well-established data governance structures—including DPIAs, committees, and internal policies—are valuable assets for AI governance. However, their reuse requires methodological and ethical adjustments tailored to the specific challenges of algorithmic systems.

Furthermore, we explored how DPIAs and AIAs complement each other, providing robust foundations for mapping, mitigating, and justifying risks related to privacy and systemic AI effects. The integration of these instruments strengthens accountability and institutional trust.

We broadened the scope of legal protection: although the starting point remains the data subject, it is recommended—especially in high-risk contexts—to consider the possible impacts on any person affected by automated decisions. In this regard, AI governance evolves to include, in addition to data protection, broader concerns such as human dignity, non-discrimination, and social justice.

In this scenario, the DPO and CAIO are not competitors; they are strategic partners. Each, from their respective domain, contributes to ensuring that AI is technically robust, legally sound, socially legitimate, and ethically defensible.

The future of AI in Brazilian organizations will be shaped not only by the ability to innovate but also by the maturity to govern responsibly, with trust and purpose. A well-prepared DPO will be a key figure in this process—not to hinder innovation, but to enable it in a fair, auditable, and human-centered way. It is the law driving innovation with ethics and effectiveness.

Ethical and responsible AI governance reduces regulatory and reputational risks; anticipates regulatory trends; increases operational efficiency and the quality of automated decisions; strengthens institutional reputation; attracts and retains talent; builds stakeholder, customer, investor, and societal trust; and drives safe, sustainable, and socially aligned innovation with ESG goals.

*****

Complementary materials:

- Responsible AI in Data
- Why Govern AI in a Regulatory Uncertainty Scenario
- The Future of Privacy
- AI and Civil Liability of Agents
- EU AI Act: Interactive Map of Obligations and Risk Categories
- The DPO and Its Relevance to Organizations

Notes and References

[1] The AI Index Report 2025 was conducted between January and February 2025, collecting responses from 1,500 organizations with at least $500 million in annual revenue, across 20 countries and 19 sectors.

[2] Gen AI Adoption Index. These findings are based on research conducted by Access Partnership in collaboration with Amazon Web Services (AWS). IT decision-makers involved in technology investment and implementation were surveyed in over 3,739 organizations across nine countries — United States of America (USA), Brazil, Canada, France, Germany, Japan, India, South Korea, and the United Kingdom (UK). In Brazil, 411 IT decision-makers were interviewed. **Available here**.

[3] "Winning the Race - AMERICA'S AI ACTION PLAN," July 2023. **Available here**.

[4] Gartner, Inc. survey with more than 1,800 executive leaders, June 2024. **Available here**.

[5] **Available here**.

[6] AI Governance Profession Report 2025. Published by IAPP and Credo AI. The report is based on two data sources, primarily the IAPP's annual governance survey conducted in Spring 2024. More than 670 professionals from 45 countries and territories participated, responding to demographic questions about organizational size and revenue, along with 25 specific questions about AI governance. The survey aimed to evaluate institutional practices, governance structures, and the level of confidence respondents had in their organization's adopted approaches. **Available here**.

[7] CENTRE FOR INFORMATION POLICY LEADERSHIP (Hunton Andrews Kurth LLP). Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework. February 2024. **Available here**. Accessed on: July 20, 2025.

[8] **Available here**.

[9] ANPD. Guidance on the Role of the Data Protection Officer. December 2024. **Available here**.

[10] PALLARDY, Carrie. How will the role of Chief AI Officer evolve in 2025? InformationWeek, April 18, 2025. **Available here**. Accessed on: July 18, 2025.

[11] Legislative incidence recommendations in AI regulatory bills in Brazil, focused on Bill No. 2338/2023. Technical Note No. 16/2023/CGTP/ANPD. **Available here**.

[12] Governance Professio AI n Report 2025 – from page 19.

[13] Fundamental Rights Impact Assessment. Legal obligation established under Article 27 of the EU AI Act.

[14] According to the Technical Note No. 16/2023/CGTP/ANPD on AI regulation in Brazil, focused on Bill No. 2338/2023. **Available here**.

[15] IAPP; EY. Annual Privacy Governance Report 2023: Executive Summary. 2023. **Available here**. Accessed on: July 20, 2025.

[16] MASLEJ, Nestor et al. The AI Index 2025 Annual Report. Stanford: AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, 2025. **Available here**. Accessed on: April 15, 2025.

[17] As per the version of the bill approved by the Brazilian Senate on December 10, 2024.

[18] LAPIN – Laboratory of Public Policy and Internet. Report on the Regulatory Framework for Artificial Intelligence in Brazil. Brasília: LAPIN, April 2023. **Available here**. Accessed on: July 18, 2025.

[19] According to the Technical Note No. 16/2023/CGTP/ANPD on AI regulation in Brazil, focused on Bill No. 2338/2023. **Available here**.

[20] Court of Justice of the European Union. Judgment of the Court (First Chamber) of 7 December 2023 — OQ v Land Hessen (Case C-634/21, SCHUFA Holding (Scoring)). Official Journal of the European Union, C series, no. 913, of 29.1.2024. **Available here**. Accessed on: July 20, 2025.

CHECKLIST
THE ROLE OF THE DPO IN AI GOVERNANCE

1. DISTINCTIONS AND SYNERGIES BETWEEN THE DPO AND THE CAIO

a) Independence and Conflict of Interest

- ☐ My current responsibilities do not include operational decisions on AI (models, criteria, or implementation).
- ☐ There is a formal and documented assessment of the absence of conflict of interest, as required by the ANPD[1].
- ☐ If I perform other roles, they do not affect my impartiality as a DPO.
- ☐ I have the technical autonomy to issue opinions contrary to the AI strategy, if necessary.

b) Structure and Reporting

- ☐ My role is formally documented, with clear scope and responsibilities.
- ☐ I report directly to Senior Management or the Board.
- ☐ I participate in risk committees but do not have executive responsibility over AI.

c) Collaboration with the CAIO and Other Stakeholders

- ☐ Structured collaboration processes exist with the CAIO and technical areas.
- ☐ AI governance includes fundamental rights, privacy, and explainability.
- ☐ I participate in Algorithmic Impact Assessments (AIAs) involving personal data or data subject rights.

d) Model Proportional to Organizational Size and Maturity

- ☐ The current structure (role accumulation or separation) was adopted based on a formal analysis of the organization's size, budget, risks, and digital maturity.
- ☐ In the case of role accumulation, safeguards such as independent reporting, external validation, or periodic review were adopted.
- ☐ I have structured a mechanism to review the organizational structure as risks and projects evolve.

e) Training and Continuous Updates

- ☐ I receive continuous training on AI, algorithmic risks, and regulation (AI Act, LGPD, GDPR, ISO 42001, among others).
- ☐ I monitor regulatory decisions and best practices related to the DPO role and its interface with AI governance.

2. CONVERGENCE BETWEEN DATA PROTECTION AND AI GOVERNANCE STRUCTURES

a) Integrated Governance Structure

- ☐ The organization has an institutional program that encompasses personal data and AI in an integrated manner.
- ☐ There is a multidisciplinary committee for decisions on ethics, risk, and AI, with a structured and approved regulation.
- ☐ DPIAs are used as a basis for drafting AIAs.
- ☐ Data governance policies include specific guidelines for automated systems.

b) Strategic Communication and Transparency

- ☐ Communications explain, in clear and accessible language, the use of AI and the automated criteria.
- ☐ Privacy notices include specific references to the purpose of AI.
- ☐ Service channels are prepared for AI-related requests.
- ☐ Legal design is used in materials aimed at the public, promoting a fundamental understanding of algorithm use.

c) Reuse of Structures and Tools

- ☐ The privacy committee also addresses ethics and AI risk.
- ☐ Training includes topics such as bias, explainability, algorithmic accountability, and ethical AI use.
- ☐ Contracts with third parties include clauses on AI, audits, and risk mitigation.
- ☐ The organization conducts technical and ethical due diligence on third parties that develop or operate AI solutions.

d) Sustainability and Organizational Maturity

- ☐ The AI structure reuses processes and resources from data governance.
- ☐ There is a budget and team (dedicated or shared) for responsible AI initiatives.
- ☐ The DPO is involved from the beginning of AI projects involving personal data, contributing to risk assessment and defining ethical and legal safeguards.
- ☐ The adopted model respects the stage of digital maturity and is reviewed as projects and associated risks evolve.

3. DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND ALGORITHMIC IMPACT ASSESSMENT (AIA)

a) Integrated Application

- ☐ I am clear on when to use DPIA, AIA, or both.
- ☐ The documents are integrated or complementary, avoiding rework and scope gaps.

- [ ] In AI projects involving personal data, I always consider LGPD requirements, in addition to guidelines from the AI Act, Bill 2.338, and other governance frameworks.

b) Methodology and Participation

- [ ] A formal methodology exists for conducting DPIAs and AIAs, with defined stages, responsibilities, and criteria.
- [ ] Evaluations involve multidisciplinary participation: legal, technical, information security, and data science.
- [ ] Analyses include technical (robustness, accuracy), legal (legal basis, rights), and ethical (bias, social impact) aspects.

c) Reuse and Efficiency

- [ ] DPIAs are reused as direct input to compose or initiate AIAs.
- [ ] The team is familiar with reference models (NIST AI RMF, OECD AI Principles, ISO/IEC 42001) and applies them as needed.
- [ ] There is an organized record of assessments carried out, with lessons learned and a monitored action plan.

d) Limitations and Corrective Actions

- [ ] Limitations of each type of assessment are mapped, and complementary actions are adopted (e.g., simulations and external reviews).
- [ ] There is a procedure for periodic review of DPIA and AIA documents, especially after changes to AI models.
- [ ] The organization can document and justify why an assessment was conducted or waived.

4.RIGHTS OF DATA SUBJECTS AND INDIVIDUALS AFFECTED BY AI

a) Understanding and Scope

- [ ] I recognize that not all AI impacts are limited to personal data protection.
- [ ] Policies and reports also consider indirectly affected individuals, even if not data subjects under the LGPD.
- [ ] Impact assessments address social, ethical, and collective risks, in addition to legal risks.

b) Transparency and Communication

- [ ] Communications about AI use are clear regarding decision criteria, logic, and potential effects.
- [ ] There is an option to request human review of demonstrably high-impact automated decisions.
- [ ] Simple language, Legal Design, and educational strategies are used.

c) Exercise of Rights

- [ ] Service channels consider both data subjects and any individual affected by AI.
- [ ] Effective mechanisms exist for the review, contestation, and clarification of automated decisions.
- [ ] Data subject rights are adapted to algorithmic realities (explainability, proportionality, and non-discrimination).

d) Collaborative Governance

- [ ] DPO and CAIO act jointly in cases with the potential to affect fundamental rights broadly.
- [ ] The governance committee considers impacts on vulnerable groups.
- [ ] Clear protocols exist for responding to complaints, adverse effects, or unanticipated outcomes, as well as security incidents.

ABOUT US

VLK Advogados sees law as a tool to drive innovation, business success, and a more prosperous and just society.

We actively participate in the development of regulatory frameworks and hundreds of innovative projects, which allows us to anticipate trends and provide legal security to enable business in the following areas:

- Ethical Governance and Data Protection
- Artificial Intelligence
- Cybersecurity and Incident Response
- Creative Economy, Legal Marketing, and Intellectual Property
- Legal Design and Visual Law
- Advocacy and Strategic Technology Regulation
- Strategic Litigation

AUTHORS

Rony Vainzof
rony@vlklaw.com.br

Giovanna Milanese
giovanna.milanese@vlklaw.com.br

Caio Lima
caio@vlklaw.com.br

Paulo Sarmento
paulo.sarmento@vlklaw.com.br

Ingrid Soares
ingrid.soares@vlklaw.com.br

E-book "The role of the DPO in AI Governance", from August, 2025.

CC BY-ND - This license allows copying and distribution of the material in any medium or format only in an unaltered form and only if attribution is given to the creator. The license allows commercial use.