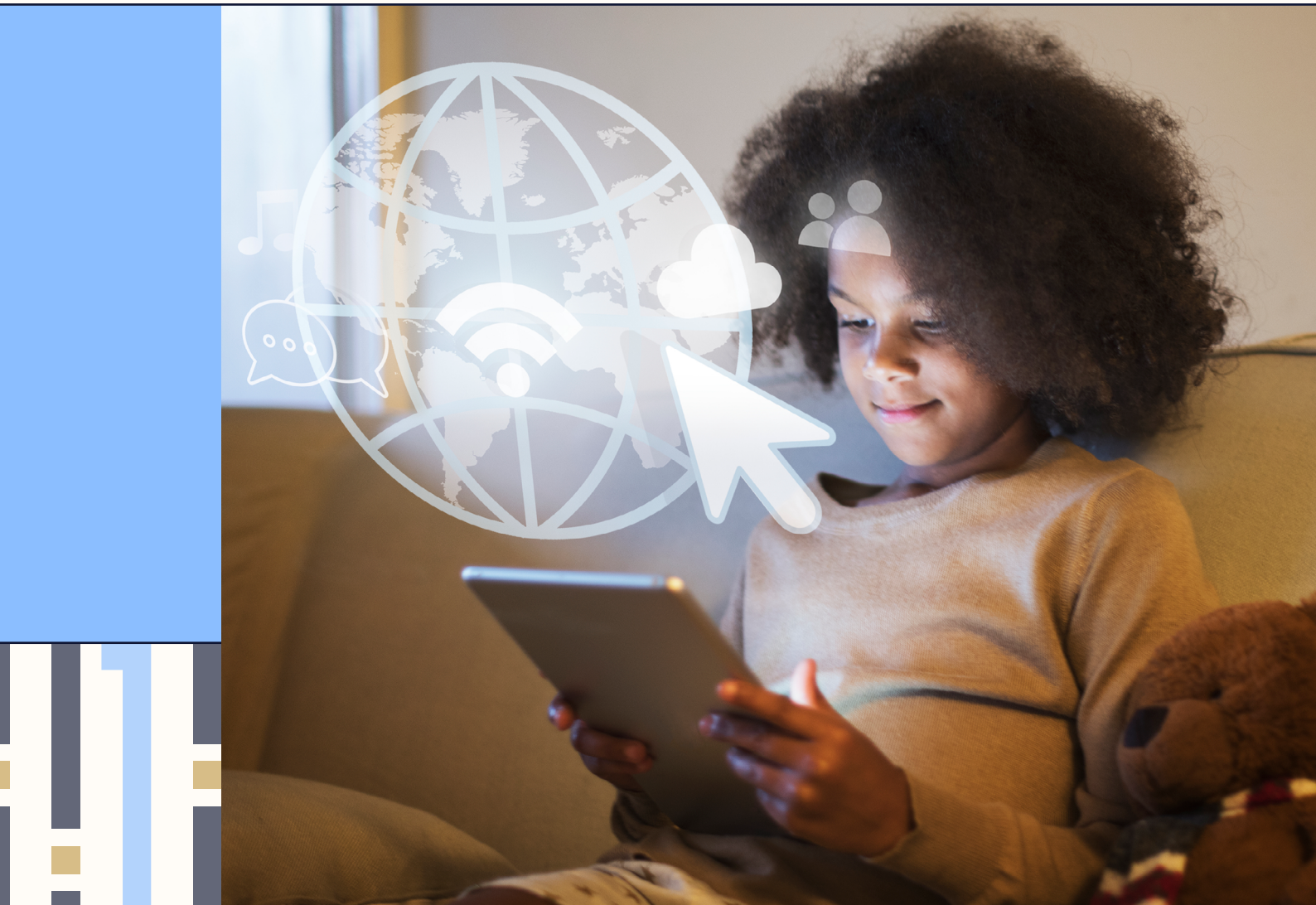
HERZOG
HERZOG FOX & NEEMAN

November
2026

Brazil's ECA Digital: Key Child Protection Obligations for Digital Products and Services

Herzog's Practical Guide



Brazil's ECA Digital

Herzog's Practical Guide



1 Introduction

Brazil's Digital Act for Children and Adolescents, Law No. 15,211/2025 (the "**Act**". Also known as the "ECA Digital", which stands for Estatuto da Criança e do Adolescente), entered into force on 17 March 2026. It establishes **preventive child protection obligations for providers of digital products and services**, supplementing Brazil's existing child protection, consumer protection and data protection frameworks. The National Data Protection Agency ("**ANPD**") is responsible for overseeing the Act.

The Act is further implemented by Decree No. 12,880/2026 (the "**Decree**"), which provides additional requirements and guidance on several key areas, including age assurance, parental supervision, digital advertising, gaming, AI systems and the protection of minors from harmful online practices.

On 28 October 2026, the ANPD published its guidance on the Act's scope and general duties relating to prevention, protection, information and security (the "**Guidance**"). The Guidance addresses key interpretative issues, including the definition of an IT product or service, when a service is considered likely to be accessed by minors, and the scope of providers' general prevention obligations.

This guide helps companies offering digital products and services in Brazil assess whether the ECA Digital applies to them and identify the steps they should take to comply. Drawing on the Act, its implementing decree and the ANPD's guidance, it explains **how to assess** whether a service is likely to be **accessed by children** or adolescents and outlines the **main obligations**, including **age assurance**, **parental supervision** and **safeguards** for **advertising**, **gaming** and **AI features**. It also covers **registration** and **reporting** requirements and sets out practical steps for providers.

2 Scope and Application

The ECA Digital applies to information technology products and services supplied remotely, electronically and at the individual request of a user, **where they are directed at children or adolescents in Brazil** or are **likely to be accessed by them**.

The Act applies **regardless of the provider's location** or where the product or service is developed, manufactured, offered, marketed or operated. Its scope is not limited to services designed for minors and may include **games**, **applications**, **messaging services**, **video-sharing** and **user-generated content** (UGC) platforms, **app stores**, **operating systems**, **online marketplaces** and other digital services.

Under the Act, "**likely access**" requires three cumulative criteria: (i) a sufficient **probability** of use and attractiveness to children or adolescents; (ii) considerable **ease of access** and use; and (iii) **a significant degree of risk** to their privacy, safety or biopsychosocial development.



The Guidance confirms that certain categories identified in the Act and Decree are **presumed likely to be accessed by minors**. These include social networks, app stores, operating systems, editorially controlled services, electronic games, providers of adult content, generative AI systems and e-commerce platforms facilitating the purchase or sale of products or services prohibited to minors. Providers within these categories generally need not conduct the ordinary likely-access assessment, unless they seek to rebut the presumption through a reasoned, case-specific assessment demonstrating that one or more statutory criteria are not met, consistently with the best interests of children and adolescents.

For ease of reference, the flowchart below provides an English translation of the "likely access" assessment set out in Annex III of the Guidance:

Annex III

Likely Access Test

Figure 6: *Flowchart for characterizing likely access for the purposes of applying the ECA Digital.*

START

Does the provider offer an information technology product or service?
- NO → The ECA Digital does not apply.
- YES ↓

Does the provider expressly state that the product or service is aimed at children and adolescents?
- YES → Application of the ECA Digital.
- NO ↓

Does the provider fall within any of the categories presumed to involve likely access or targeting (ECA Digital and Decree No. 12,880/2026)?
- NO → Carry out a likely access analysis.
- YES → Presume likely access or targeting, unless evidence demonstrates otherwise.

The three requirements of Article 1, sole paragraph, must be met cumulatively.

1. Sufficient probability of use and attractiveness of the product or service for children and adolescents.
2. Considerable ease of access to and use of the product or service by children and adolescents.
3. A significant degree of risk to the privacy, safety or development (biopsychosocial) of children and adolescents.

Respecting the principle of the best interests of the child and the adolescent (Article 4).

- YES → The product/service is subject to likely access. The ECA Digital applies.
- NO → It is not characterized as likely access under the ECA Digital.

Indicators that may support the analysis of the requirements

Availability of products or content of interest to children and adolescents.	Similarity with services considered to involve likely access under the ECA Digital and Decree No. 12,880/2026.
Use of design elements that are attractive to children and young people.	Actual access or use by children and adolescents, according to available evidence (platform data, independent research and studies).
Advertising aimed at children and adolescents.	

Categories Presumed to Involve Likely Access or Targeting

- Social networks
- Application stores
- Operating systems
- Services with editorial control
- Electronic games
- Adult content providers
- Generative artificial intelligence systems
- E-commerce platforms that intermediate the purchase and sale of products and services prohibited for children and adolescents

IMPORTANT

The provider's self-assessment does not bind the ANPD, which may, based on the legal criteria, the principle of the best interests of the child and the adolescent and the specific characteristics of the product or service, reach a different conclusion and determine compliance with the ECA Digital, including the additional protective measures set out in Articles 34 and 39. The application of the Law does not depend solely on the provider's declaration or on formal classifications made by the target audience.

Differentiated treatment: The obligations provided for in Articles 6, 17, 18, 19, 20, 27, 28, 29, 31, 32 and 40 of the ECA Digital apply in accordance with the characteristics and functionalities of the information technology product or service, adjusted to the degree of interference of the product or service provider over the available content, the number of users and the size of the provider.



The assessment must reflect the product's or service's **actual characteristics and conditions of use**, not merely its declared target audience. Illustrative indicators include:

Products or content of interest to minors;

Appealing design and engagement features;

Advertising directed at them;

Similarities to services presumed likely to be accessed by minors; and

Evidence of actual use

These indicators are not additional legal requirements and do not replace the three cumulative criteria; no single indicator is determinative. Accordingly, an "18+" designation does not, by itself, exclude a service from the Act. Nor can age assurance measures adopted to comply with the Act be relied upon to negate likely access, as applicability must be determined before assessing compliance.

The Guidance calls for a **proportionate, risk-based approach** to implementing the Act. Relevant factors include the product's or service's nature and risks, its business model, the provider's influence over available content, the number of users and the provider's size. These factors inform the form and extent of required measures; they do not create a general exemption from the Act.





3 Main Compliance Requirements

Safety by Design, Privacy by Default and General Prevention Duty

The ECA Digital establishes a general duty of prevention, protection, information and security. This includes specific requirements, including adopting reasonable measures from the design stage and throughout the operation of digital services to prevent and mitigate risks to minors, applying the highest available level of privacy and personal data protection by default, and implementing measures to prevent excessive, problematic or compulsive use. The measures required should reflect the nature, functionality and risks of the relevant service.

Child Safety and Health Impact Assessment

According to the Decree, providers whose products or services are directed at or likely to be accessed by minors must conduct an impact assessment addressing children's safety and health. The assessment must identify and analyze relevant risks, evaluate their likelihood and potential severity, establish mitigation measures and continuously monitor their effectiveness. A summary must be made publicly available in clear and accessible language. The ANPD may establish additional requirements.

Age Assurance and Age Verification

Providers must adopt age-assurance measures proportionate to the risks associated with their services, taking into account accuracy, reliability, robustness, privacy and security. More stringent age-verification requirements apply to content, products and services whose access is prohibited or inappropriate for minors, particularly pornographic content. Self-declaration alone is insufficient where reliable age verification is required. Providers making pornographic content available must also prevent minors from accessing such content, including by hiding, blurring or withholding pornographic images and videos by default, or requiring age verification to unlock access.



Brazil's ECA Digital

Herzog's Practical Guide



Age Signals from App Stores and Operating Systems

App stores and operating systems must implement proportionate, auditable and technically secure age-assurance measures, provide parental supervision tools and make age signals available to application providers through secure, privacy-preserving APIs. These signals must be limited to information necessary to confirm whether a user meets the relevant age threshold, without disclosing unnecessary information such as an exact date of birth or civil identity. App stores and operating systems must also obtain parental or guardian authorization before minors download and install applications and provide the relevant age-rating information before authorization.

Providers of covered digital services must implement technical and organizational measures to ensure receipt of age information and, where their services offer content, products or services inappropriate or prohibited for minors, must receive the relevant age signals. However, age signals do not replace providers' own responsibility to implement effective age-appropriate safeguards. Providers must independently adapt their services to the user's age and prevent access to inappropriate content. Services accessed through web browsers must implement their own age-assurance mechanisms, although they may rely on age signals provided by operating systems, app stores or other digital service providers.

Parental Supervision

Relevant providers must offer accessible parental-supervision tools enabling parents or legal guardians to manage children's account and privacy settings, restrict purchases and financial transactions, identify adult profiles with which their children communicate, and monitor consolidated metrics of total usage time. Such tools and related information must be clear, accessible and available in Portuguese.

Account Linkage and Social Networks

Providers of digital products and services directed at or likely to be accessed by minors must ensure that accounts operated by children and adolescents aged 16 or younger are linked to a parent's or legal guardian's account. Separately, social networking services that are inappropriate for minors must adopt additional safeguards, including clear and prominent notices that the service is unsuitable for minors, measures to restrict content evidently intended to attract minors, and continuous improvement of age-verification mechanisms to identify accounts operated by underage users.

Local Legal Representative

Providers of products or services within the scope of the Act are required to maintain a legal representative in Brazil.



Content Moderation and User Reporting

Providers must maintain accessible mechanisms for users to report content that violates the rights of children and adolescents. In specified circumstances, providers must promptly remove such content following a qualifying notice from an authorized notifier, without awaiting a court order. Relevant moderation decisions must be reasoned and subject to appropriate appeal mechanisms, in accordance with the Act's statutory conditions and exemptions. Separate reporting, removal and preservation obligations applicable to specified serious violations are discussed in the next section.

Advertising and Monetization Restrictions

The Act prohibits the use of profiling, emotional analysis, augmented reality, extended reality and virtual reality techniques to target commercial advertising at minors. It also prohibits creating behavioral profiles of minors for commercial advertising purposes. In addition, the Act prohibits monetizing or promoting content portraying minors in an eroticized or sexually suggestive manner or in an adult sexual context.

AI Systems and Conversational Agents

Providers of digital products or services directed at or likely to be accessed by minors that are capable of generating content and interacting with users based on natural language instructions, including large language models and conversational agents, must: (i) disclose the synthetic and automated nature of interactions with minors; (ii) prevent behavioral manipulation; (iii) assess algorithmic risks to minors' safety and health; and (iv) implement safeguards to protect their physical, mental and psychosocial development. The ANPD is responsible for further regulating and supervising compliance with these requirements.

Gaming, Loot Boxes and Interactive Features

The ECA Digital prohibits loot boxes in electronic games directed at or likely to be accessed by minors, in accordance with the applicable age classification. Loot boxes are paid features that allow players to acquire consumable virtual items or random advantages without knowing their contents in advance or being guaranteed their actual utility. Providers must verify users' ages to prevent minors from accessing loot-box features, unless the game offers a version without loot boxes or completely restricts access to those features by default.

Separately, games enabling user interactions through text, audio, video or content sharing, whether synchronously or asynchronously, must implement the applicable moderation and user-protection safeguards and, by default, limit such interactions to ensure parental or guardian consent.



4 Nidus Registration and Reporting Obligations

Nidus is the Federal Police system for receiving and processing reports of specified serious violations involving minors, operated through the CNCA. Under the Federal Police Ordinance No. 19,107/2026 (the "**Ordinance**"), registration is **mandatory** where both of the following conditions are met:

a. since 17 March 2026, the provider has identified, in its products or services, any of the reportable violations described under "reporting scope" below; **and**

b. the provider **either**

   i. offers products or services directed at or likely to be accessed by minors in Brazil, **or**

   ii. provides pornographic content, escort services or services facilitating sexual encounters or relationships, even if minors are not the intended or likely audience.

Registration is also **recommended** for providers within these categories that have not identified reportable incidents but consider that such incidents may occur. Other providers may register voluntarily, without this alone constituting an admission that the Act applies.

Providers subject to mandatory registration must complete the process by 19 December 2026.

Registration and reporting are separate: reporting, removal and preservation obligations apply even without registration, and reporting to foreign centers does not exempt a provider from registering in Brazil. However, a duplicate report to the CNCA is not required where an identical report submitted to a foreign reporting center is accessible to Brazilian authorities.

Reporting scope. The Act and the Decree require providers of IT products or services available in Brazil to report specified violations detected through their products or services, including: (i) content evidencing criminal or infringing conduct involving the sexual exploitation, abuse or grooming of a child or adolescent; (ii) kidnapping or unlawful confinement; and (iii) content or interactions evidencing the grooming, recruitment or coercion of a child or adolescent for conduct presenting a credible, imminent or ongoing risk of serious physical injury or death, including child trafficking and preparations for extreme premeditated violence against school communities or vulnerable groups.

Reports must be submitted:



Within 12 hours

where there is a credible, imminent or ongoing risk to a child or adolescent.

Within 72 hours

for other cases involving indications of child sexual abuse material that was produced recently (within the preceding 90 days), has not previously been identified in the provider's reference databases, or was produced using a capture tool made available by the provider.

Within seven days

for other qualifying incidents



Reports should include available relevant information, such as incident details, associated accounts, content, URLs and technical data. Providers must immediately remove material relating to the specified reportable violations from user access. The material, related account information and metadata must be preserved, in a restricted and secure environment and solely for this purpose, for submission to the CNCA or a competent international authority, as applicable, subject to applicable retention requirements.

Report submission through Nidus is not yet operational and awaits a further Federal Police ordinance, following which providers will have up to 120 days to adapt to these deadlines. The existing duties to remove and preserve identified material continue to apply in the meantime.

5 Exceptions and Limitations

Exemptions for Editorially Controlled and Licensed Content

The Act provides limited exemptions from certain obligations for services that exercise genuine editorial control over their content and services providing copyright-protected content licensed in advance from a responsible economic agent other than an end user. These exemptions are subject to specific statutory conditions and do not constitute a general exemption from the Act.

Exemption from Age Assurance

In addition, the Decree provides an exemption from age-assurance requirements for certain editorially controlled services and services providing pre-licensed copyright-protected, musical or literary content, subject to conditions relating to child-appropriate accounts or profiles, parental supervision and access restrictions. Editorially controlled news and sports services that are not subject to age classification are also exempt from age-assurance requirements.

Application to UGC Platforms

The Guidance clarifies that editorial control requires the prior selection and curation of content through human assessment. Merely hosting, recommending, ranking or moderating user-generated content does not qualify. Importantly, the exemptions apply based on the nature of the service as a whole, rather than individual content items. Accordingly, a UGC platform does not qualify merely because it hosts professionally produced or licensed content (e.g., a licensed episode of a children's series uploaded to a video-sharing platform). Eligibility must be assessed based on the service's actual operation and the specific conditions of each exemption.



6 Enforcement and Penalties

Sanctions under Article 35 of the Act

- **Warnings** → The ANPD may issue warnings requiring companies to address identified violations.
- **Administrative fines** →
  - Fines may reach **10% of the economic group's annual revenue in Brazil** for the preceding financial year.
  - If there is no such revenue, fines may range from **R$10 to R$1,000 per registered user** of the sanctioned provider, capped at **R$50 million per violation.**
  - The Act does not limit this calculation to minors.
  - Fine amounts are subject to annual inflation adjustments.
- **Suspension or prohibition of activities** → Companies may face temporary suspension or prohibition of their activities in Brazil, subject to a court order.
- **Additional liability** → These sanctions do not exclude other potential civil, criminal or administrative liability.

Nidus registration: Ordinance No. 19,107/2026 does not establish a separate monetary penalty for failure to register with Nidus. However, failure to register does not remove the underlying reporting, removal or preservation obligations.





7 What Should Companies Do Now?

Companies operating digital products or services accessible in Brazil should consider the following:

1 Assess scope and applicability

Map products and services available in Brazil against the statutory criteria and any applicable presumption of likely access, and document the assessment and any reliance on an exemption or rebuttal

2 Identify applicable obligations

Determine which requirements apply to the relevant service and provider, including age assurance, parental supervision, account linkage, privacy-by-default settings, content moderation and local representation.

3 Conduct a child safety impact assessment

Review product design, recommendation systems, interaction features, monetization and data practices, and publish the required summary.

4 Review age-related safeguards and user protections

. Assess age-verification mechanisms, parental controls, account restrictions and safeguards against exposure to inappropriate content.

5 Review advertising, AI and gaming features

Assess applicable restrictions on targeted advertising, AI-generated interactions, loot boxes, virtual currencies, in-game purchases and user interaction features.

6 Assess Nidus registration requirements

Determine whether mandatory registration applies based on reportable incidents identified since 17 March 2026, and register by 19 December 2026 where required.

7 Establish reporting and preservation procedures

Review detection, escalation, removal, reporting and evidence-preservation processes ahead of the Nidus reporting launch.

8 Monitor regulatory developments

Track the further Federal Police ordinance governing report submission and additional ANPD regulations and guidance.

Please feel free to contact us if you have any questions about how the ECA Digital applies to your products or services or would like assistance with your compliance efforts.



HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique combination of **legal**, **technological** and **operational** expertise, and is uniquely positioned to advise a wide range of clients, including leading multinational technology companies as well as start-ups and vendors of disruptive technologies, on regulatory and compliance considerations across the digital ecosystem.

We understand that companies operating in digital environments face regulatory scrutiny that extends far **beyond one jurisdiction or discipline**. As our clients are often at the forefront of rapidly evolving markets, we recognize the impact that **global enforcement trends, platform rules and design-related compliance requirements** have on their products and operations. Our team maintains in-depth knowledge of the growing body of regulation, enforcement actions and industry standards that govern online interfaces, user journeys and commercial communications. This enables us to offer practical and holistic solutions for complex situations arising from innovative technologies and fast-moving regulatory expectations.

Digital products, online platforms, eCommerce, advertising and user-facing interfaces now form a core component of almost every business. Advising on these issues requires deep understanding of the intersection between legal requirements, UX and UI design practices, behavioral economics, product architecture and commercial strategy. We help clients navigate interdisciplinary and sometimes conflicting obligations that arise under privacy, consumer protection, online safety and advertising laws together with platform guidelines and industry codes.

Our dark-patterns and interface-design advisory support spans the full lifecycle of product development and ongoing operations. This includes:

- Analyzing product flows and user journeys to identify potential dark patterns, deceptive design risks and areas of regulatory exposure;
- Advising on global regulatory requirements related to interface design, including restrictions on manipulative, misleading or high-friction patterns;
- Designing and documenting defensible, user-centric and regulator-aligned decision flows that promote transparency and informed choice;
- Supporting teams in structuring clear notices, consent mechanisms and commercial communications that withstand regulatory scrutiny;
- Developing governance frameworks and internal processes that integrate dark-patterns compliance into product, engineering, design and marketing workflows;
- Assisting with regulatory engagement, including responses to inquiries, investigations and enforcement actions involving deceptive or manipulative design allegations.

This document does not constitute an exhaustive legal opinion or regulatory overview of all applicable regulatory requirements regarding the topics addressed by it, but rather, only outlines the key issues arising from the regulatory requirements. Since we are not licensed to practice law outside of Israel, this document is intended to provide only a general background regarding this matter. This document should not be regarded as setting out binding legal advice, but rather a general overview which is based on our understanding of the practical interpretation of the applicable laws, regulations and industry guidelines.

HERZOG
HERZOG FOX & NEEMAN

Brazil's ECA Digital

Herzog's Practical Guide





Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il



Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il



Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il



Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il



Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il



Dima Zalyalyeyev | Partner
Technology Regulation
zalyalyeyevd@herzoglaw.co.il



Or Noy | Partner
Technology Regulation
noyo@herzoglaw.co.il



Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il



On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il



Tal Habas | Associate
Technology Regulation
habast@herzoglaw.co.il



Zohar Malul | Associate
Technology Regulation
malulz@herzoglaw.co.il



Tali Torigian | Associate
Technology Regulation
torigiant@herzoglaw.co.il



Omri Bar On | Associate
Technology Regulation
barono@herzoglaw.co.il



Adaya Ziv-Kisos | Associate
Technology Regulation
Zivkisosa@herzoglaw.co.il



Liron Adar | Associate
Technology Regulation
adarl@herzoglaw.co.il



Eden Lapid | Associate
Technology Regulation
lapide@herzoglaw.co.il



Yuval Glazer | Associate
Technology Regulation
glazery@herzoglaw.co.il



Gal Mechtinger | Associate
Technology Regulation
mechtingerg@herzoglaw.co.il



Tal Schapiro | Associate
Technology Regulation
schapirot@herzoglaw.co.il



Clara Qubti | Associate
Technology Regulation
qubtyc@herzoglaw.co.il



Roni Sharir | Intern
Technology Regulation
sharirR@herzoglaw.co.il



Korin Arbel | Intern
Technology Regulation
arbelk@herzoglaw.co.il



Tamar Oppenheim | Intern
Technology Regulation
oppenheimt@herzoglaw.co.il



Itay Siani | Intern
Technology Regulation
sianii@herzoglaw.co.il



Noya Schwartz | Pre-intern
Technology Regulation
schwartzn@herzoglaw.co.il



Max Shternberg | Pre-intern
Technology Regulation
shterenbergm@herzoglaw.co.il



Musa Assi | Law Student
Technology Regulation
assim@herzoglaw.co.il