/AURUM

World Mini Apps

Developer Legal Guidelines

2026

Contents

Introduction 4

1. How to Use This Guide 5

2. Legal and Regulatory Framework 6

2.1 Applicable Rules 6

2.2 Regulated Activities & Jurisdictional Restrictions 6

Payments and Financial Services Regulation

Securities and Investment Services Regulation

Crypto Assets Regulation

Gaming and Gambling Regulation

2.3 World App Rules 12

3. Operating Requirements 13

3.1 Corporate Structure 13

3.2 Terms & Conditions 15

3.3 Taxation 16

4. Payments 16

4.1 Crypto Assets 16

4.2 Fiat Payments 16

5. Privacy and Data Protection 16

5.1 Data Protection Regimes 17

5.2 Personal Data 17

5.3 High-Level Obligations in Relation to Personal Data 17

5.4 Transparency and User Notices 17

5.5 Data Minimisation, Security, and Retention 17

5.6 SDKs, Analytics, Cookies, and Third-Party Integrations 17

6. Consumer Protection 18

6.1 General 18

6.2 Refunds 18

6.3 Unfair Commercial Practices 19

7. Intellectual Property Basics 20

7.1 Why Intellectual Property Matters for Mini Apps 20

7.2 Copyright: Code and Content 20

7.3 Trademarks and Brand Assets 20

7.4 Third-Party Code 21

7.5 User-Generated Content 21

7.6 Ownership and Assignment of IP 21

8. Q&A 23

References 26

Contributors 27

Introduction

The World ecosystem is a multi-layered project[1] developed to support human-centric digital identity, financial access and decentralised infrastructure. The World ecosystem combines digital identity (World ID), a blockchain network (World Chain), a digital token (Worldcoin) and the World App itself. Mini Apps are applications that run inside World App, functioning similarly to apps distributed through traditional app stores.This ecosystem demonstrates significant global adoption and continues to grow rapidly across regions and use cases, with more than 38.3 million users (including 17.8 million verified users) as of February 2026[2].

This guide covers the main legal and compliance requirements for building Mini Apps on World App — from initial development through launch and ongoing operation. The focus is on legal and regulatory requirements only. Technical implementation, World ID and World Chain are outside the scope of this guide.

We hope this guide serves as a practical blueprint for founders building within the World ecosystem, helping teams identify the key legal and compliance considerations early and navigate them as they scale.

This guide is for informational purposes only and does not constitute legal advice. For guidance specific to your project, consult a qualified professional.

> *"Mini Apps are applications that run inside World App, functioning similarly to apps distributed through traditional app stores."*

/AURUM

Legal partner behind the builders of tomorrow ©

1. How to Use This Guide

This guide covers a wide range of legal topics – not all of them will apply to every Mini App. Rather than reading the document from start to finish, we recommend the following approach:

Start with Section 2 (Legal and Regulatory Framework). Read the overview paragraphs in each subsection to determine whether your Mini App involves regulated activities — such as payments, securities, crypto assets or gaming. If a category does not apply to your product, you can skip the detailed subsections.

Read Section 3 (Operating Requirements) in full. Corporate structure, terms and conditions, and data protection are relevant to virtually every Mini App, regardless of its functionality.

Consult Sections 4-7 as needed. These sections cover taxation, advertising, consumer protection and intellectual property. Use the table of contents and FAQ section to find the topics relevant to your situation.

If you are unsure whether a particular regulation applies to your Mini App, treat it as potentially applicable and seek professional legal advice. This guide provides general information — it does not replace jurisdiction-specific analysis.

2. Legal and Regulatory Framework

2.1 Applicable Rules

Mini Apps must comply with three layers of rules:

> *"Compliance with one layer does not automatically mean compliance with the others. Each layer operates independently and must be assessed separately."*

1. Laws and regulations of relevant jurisdictions.
2. Marketplace (App Store[3] and Google Play[4]) terms and conditions.
3. World App terms and conditions.

Compliance with one layer does not automatically mean compliance with the others. Each layer operates independently and must be assessed separately.

Local law always takes precedence over platform rules. A feature permitted by World App may still be prohibited in certain jurisdictions. For example, crypto transactions are allowed on World App but restricted in China. If a feature is unlawful in a given region, the developer must ensure it is not available to users there.

Laws and Regulations

For online businesses, determining which laws apply is more complex than for offline ones. In an online environment, several jurisdictions may apply simultaneously. In particular:

- The jurisdiction where the developer or operating company is established.
- The jurisdiction where users are located.
- The jurisdiction that is actively targeted through marketing or localised content.

For example, a Mini App developed in the UAE with a French-language interface and French-targeted advertising would generally need to comply with French law, even if some Brazilian users also access it incidentally.

Note that using blockchain technology does not, by itself, change which laws apply. Consumer and data protection regulatory frameworks apply regardless of the underlying technology.

Marketplace Rules

App Store and Google Play policies apply to World App as the distributing platform. As a result, they also affect Mini Apps. A serious violation by a Mini App may be treated as a violation by World App itself, so World App actively monitors Mini App compliance with marketplace policies.

World App Rules

World App has its own set of rules that largely mirror App Store and Google Play policies but also include platform-specific restrictions. For instance, Mini Apps may not use the word "World" in their name. These rules are covered in detail in the "World App Rules" section below.

Mini App Rules

Developers may also set their own rules for users (terms and conditions, privacy policies, etc.), provided these do not conflict with any of the above. See the "Terms & Conditions" section for details.

2.2 Regulated Activities & Jurisdictional Restrictions

> *"Regulation may apply even where decentralised infrastructure, open-source protocols or smart contracts are used. Regulators assess substance and economic function rather than technical architecture."*

Overview

Mini Apps are subject to a broad range of laws and regulations. In addition to generally applicable regimes, such as tax, consumer protection, data protection and advertising rules, certain Mini Apps may fall within sector specific regulatory frameworks.

In practice, the most relevant regulatory considerations for Mini Apps distributed via the World App arise where a Mini App enables or facilitates activities involving financial risk or chance-based outcomes.

As a practical rule of thumb, Mini Apps are most likely to trigger sector-specific regulation where they involve:

- Payments or other financial services;
- Crypto assets or token-based functionality;
- Securities or investment-like features; or
- Gaming, gambling, or prize-based mechanics.

Whether a Mini App is regulated depends on its specific features and how they are implemented. Functionality that may appear technical or entertainment-focused – such as enabling payments, distributing tokens, facilitating trades or offering reward-based games – can fall within existing regulatory definitions in certain jurisdictions. Developers should be aware that user interactions, monetisation models and the ability to transfer, store or exchange value are particularly relevant factors.

Regulatory outcomes vary significantly by country. A particular activity may be unregulated in one jurisdiction but require formal licensing, ongoing compliance obligations (including KYC/AML measures) or outright prohibition in another.

This section therefore outlines the most common categories of regulated activities relevant to Mini Apps and provides high-level guidance on when developers may need to consider licensing, registration, user verification measures, or jurisdiction-based access restrictions.

Payments and Financial Services Regulation

When Regulation May Apply

A Mini App may fall under payment or financial services regulation when it enables users to:

- Transfer money or monetary value.
- Store value, including user balances.
- Initiate payment transactions.
- Intermediate payments for third party goods or services.
- Carry out other activities classified as regulated under applicable law.

Developers should assess whether the Mini App conducts regulated activities in the jurisdictions where it operates and where it is made available. This could include cases where the Mini App:

- Holds user funds or maintains user balances.
- Example: A wallet-like feature allowing users to store funds for later use.
- Transfers money between users.
- Example: Peer-to-peer tipping or remittances.
- Facilitates merchant payments on behalf of sellers.
- Example: A marketplace Mini App where the app provider collects payments from buyers and settles with sellers.
- Issues stored value.
- Example: Prepaid credits or reloadable balances.

Key Regulatory Frameworks

Applicable regimes may include:

- European Union: Payment Services Directive 2 (PSD2)[5].
- United Kingdom: Electronic Money Regulations[6] and the Payment Services Regulations[7].
- United States: Federal money services businesses regulations, and state-level money transmitter laws.

Regulated Activity

Where payment or financial functionality is involved, developers must decide whether to operate as a regulated provider or to avoid or outsource regulated activity.

If there is no intention to become regulated, the Mini App must be designed so that it does not perform regulated activities. This generally requires avoiding:

- Holding or safeguarding user funds;
- Maintaining user balances or stored value;
- Transmitting money between users;
- Executing payments on behalf of users;
- Enabling withdrawals or redemptions.

Where payment or financial functionality is required but the developer does not intend to be regulated directly, the most common approach is to partner with a regulated third-party provider (such as a licensed payment processor). In these cases:

- The regulated provider typically performs the regulated services in its own name under its licences.

- The Mini App acts as a technical interface.
- Core compliance obligations, including KYC and AML, are typically undertaken by the regulated partner, although contractual and operational responsibilities may still apply to the developer.

If the developer intends to provide regulated payment or financial services directly, a full compliance framework is required. This includes:

- Identifying the relevant regulated services.
- Determining the jurisdictions in scope.
- Obtaining required licences or authorisations prior to launch.
- Ensuring ongoing compliance, including KYC and AML, transaction monitoring, consumer disclosures and activity restrictions.

Securities and Investment Services Regulation

> *"A Mini App may fall under securities or investment services regulation where it enables or facilitates activities that involve investments, financial instruments, or capital markets-related services."*

When Regulation May Apply

A Mini App may fall under securities or investment services regulation where it enables or facilitates activities that involve investments, financial instruments, or capital markets-related services. Unlike payments regulation, which focuses on the movement of value, securities regulation is primarily concerned with investor protection, market integrity, and disclosure of financial risk.

A Mini App may be subject to securities or investment services regulation when it enables users to:

- Invest in, purchase, sell, or trade financial instruments.
- Participate in securities or investment product offerings.
- Receive investment-related services, such as brokerage, dealing, or portfolio management.
- Access trading venues, marketplaces, or matching mechanisms for securities.
- Receive investment advice or automated investment strategies.
- Participate in tokenised or digital representations of securities or other regulated financial instruments.

Such activities are typically prohibited unless carried out by authorised entities.

Developers should assess whether a Mini App performs regulated investment activities in the jurisdictions where it is accessible. This may include cases where the Mini App:

- Facilitates the purchase or sale of securities.
- Example: A Mini App allowing users to purchase shares, bonds, or other investment instruments.
- Operates or provides a frontend to a trading platform.
- Example: Providing a frontend for an investment marketplace or exchange.
- Intermediates investment transactions.
- Example: Matching buyers and sellers of investment products or routing orders to third-party brokers.
- Provides investment advice or recommendations.
- Example: Suggesting specific investments, portfolios, or expected returns, whether manually or via algorithms.
- Offers access to collective investment schemes or similar structures.
- Example: Investment pools, funds, or revenue-sharing arrangements.
- Enables trading or distribution of assets that are legally classified as securities, including tokenised securities or digital instruments that fall within securities definitions under applicable law.

Importantly, securities regulation focuses on substance over form. Even where an activity is framed as technological, community-based, or experimental, it may still be regulated if it performs the economic function of an investment service.

Key Regulatory Frameworks

Relevant regimes may include:

- European Union: Markets in Financial Instruments Directive (MiFID II)[8].
- United Kingdom: Financial Services and Markets Act 2000 (FSMA)[9] and related FCA rules governing

regulated investment activities.

- United States: Federal securities laws administered by the SEC, including the Securities Act[10] and the Exchange Act[11]. State-level "blue sky" laws may also apply.

Regulated Activity

If there is no intention to operate as a regulated investment services provider, the Mini App must be designed to avoid regulated activities. This typically requires avoiding:

- Enabling users to buy, sell, or trade securities.
- Matching investors with issuers or other investors.
- Presenting investment opportunities or capital-raising initiatives.
- Providing personalised or general investment advice.
- Displaying expected returns, profit projections, or performance analytics tied to financial instruments.

User interface design and marketing language are relevant to regulatory classification and must be carefully managed.

Where investment functionality is required but direct regulation is not intended, developers often integrate licensed third party brokers or investment firms. In this structure:

- The regulated provider performs the regulated investment services in its own name and under its own licence.
- The Mini App functions as a technical interface or access layer.
- Investor onboarding, disclosures, suitability assessments, and regulatory reporting are handled by the regulated provider.

As with payment services, this model requires careful structuring to ensure that the developer is not deemed to be providing regulated investment services itself.

If the developer intends to provide securities or investment services directly through the Mini App, a comprehensive regulatory strategy is required. Developers should:

- Identify the specific regulated investment services being offered (e.g. brokerage, dealing, investment advice, operation of a trading venue).
- Determine the jurisdictions in which users will access those services.
- Obtain the relevant licences or authorisations before launch.
- Ensuring ongoing compliance with securities laws, including KYC and AML, conduct of business rules, disclosure obligations and marketing restrictions.

Crypto Assets Regulation

When Regulation May Apply

A Mini App may fall under crypto assets regulation where it enables activities involving cryptoassets, digital tokens or other forms of blockchain-based value. Regulation in this area is evolving rapidly and varies by jurisdiction, but generally focuses on consumer protection, financial stability and anti-money laundering (AML).

A Mini App may be subject to crypto asset regulation when it enables users to:

- Create, issue, distribute, or redeem cryptoassets.
- Transfer cryptoassets between users or to external wallets.
- Store, manage, safeguard, or custody cryptoassets on behalf of users.
- Exchange cryptoassets for other cryptoassets or fiat currency.
- Use cryptoassets as a means of payment for goods or services.

Regulation may apply even where decentralised infrastructure, open-source protocols or smart contracts are used. Regulators assess substance and economic function rather than technical architecture.

Developers should assess whether a Mini App conducts regulated crypto asset activities in the jurisdictions where it is accessible. This may include cases where the Mini App:

- Controls or safeguards user cryptoassets.
- Example: Custodial wallets where the Mini App or developer controls private keys.
- Facilitates crypto transfers or payments.
- Example: Allowing users to send tokens to each other or pay merchants using cryptoassets.

- Provides exchange or conversion functionality.
- Example: Swapping tokens, converting cryptoassets to fiat, or routing trades through liquidity providers.
- Managing third-party cryptoassets.
- Example: Trading cryptoassets using liquidity provided by users.

Key Regulatory Frameworks

Relevant regimes may include:

- European Union: Markets in Crypto-Assets Regulation (MiCA)[12].
- United Kingdom: FCA registration under the UK's AML regime[13] for cryptoasset exchange and custody services.
- United States: Federal AML obligations under FinCEN for money services businesses involved in cryptoasset transmission, and state-level money transmitter or crypto currency laws.

These regimes typically impose registration or licensing requirements, AML obligations, consumer disclosures, and operational safeguards.

Regulated Activity

If there is no intention to operate as a regulated crypto asset service provider, the Mini App must be designed to avoid regulated activities. This may require avoiding:

- Custody or control of users' private keys.
- Facilitating crypto transfers or exchanges.
- Providing token swap or conversion functionality.
- Transferability of crypto assets.
- Offering centralised staking, yield, or similar crypto-financial services.

Certain design choices may reduce regulatory exposure. Non-custodial models, where users retain sole control of private keys, may fall outside custody regimes. Read only functionality, such as displaying balances or on chain data without enabling transactions, is less likely to be regulated. Purely informational or analytical tools, including portfolio tracking or market data, may also reduce risk where no transactions are facilitated.

However, regulators will assess the developer's actual role and the practical effect of the functionality. If the Mini App meaningfully facilitates transactions or forms part of a value transfer process, regulatory obligations may arise notwithstanding a decentralised or non-custodial design.

Where crypto functionality is required but the developer does not intend to be regulated directly, and is not willing to develop or integrate non-custodial solutions, a common approach is to integrate licensed third-party crypto service providers. In these cases:

- The regulated provider performs the cryptoasset services in its own name and under its regulatory permissions. The Mini App acts as a technical interface or access layer.
- Compliance obligations such as KYC/AML, transaction monitoring, and regulatory reporting are typically handled by the regulated provider.

This model is widely used but requires careful structuring to ensure that the developer is not considered to be providing regulated services indirectly.

If the developer intends to provide regulated crypto asset services directly, a comprehensive compliance framework is required. Developers should:

- Identify the specific cryptoasset services being provided (e.g. custody, exchange, transfer, issuance).
- Determine the jurisdictions in which those services will be offered.
- Obtain the relevant registrations or licences before launching the functionality.
- Operate the Mini App in ongoing compliance with applicable cryptoasset regulations, including KYC/AML obligations, sanctions screening, and restrictions on permitted activities.

Gaming and Gambling Regulation

> *"Gaming and gambling laws are typically enforced strictly, and in many jurisdictions gambling activities are prohibited unless conducted by licensed operators."*

When Regulation May Apply

A Mini App may fall under gaming or gambling regulation where it enables activities involving games, contests or interactive experiences in which users can obtain prizes, rewards or other items of value. This area is regulated

primarily due to concerns around consumer protection, fairness, addiction risks and protection of minors. Gaming and gambling laws are typically enforced strictly, and in many jurisdictions gambling activities are prohibited unless conducted by licensed operators.

A Mini App may be regulated where it enables users to:

- Participate in games of chance or mixed chance-and-skill.
- Stake money, tokens, or items of value to participate in a game or contest.
- Receive prizes with monetary value or that can be exchanged for value.
- Purchase or open loot boxes or similar randomised reward mechanisms.
- Participate in lotteries, raffles, prediction markets, or prize draws.
- Engage in competitive games or tournaments offering valuable rewards.

Regulators generally assess whether the activity involves some combination of:

- Consideration (payment or stake to participate),
- Chance (randomness or uncertainty in outcome), and
- Prize (something of value).

Where these elements are present, the activity is often classified as gambling, although some jurisdictions require fewer elements. For example, in some jurisdictions consideration may not be a mandatory prerequisite, and any game of chance offering a prize may be treated as gambling.

Key Regulatory Frameworks

Gambling regulation is largely jurisdiction specific:

- European Union: Primarily national regimes, with many EU Member States requiring licences for online gambling and prize-based mechanics.
- United Kingdom: The Gambling Act 2005 and UK Gambling Commission rules.
- United States: Predominantly state level laws, with significant variation. Certain activities may also trigger federal laws, particularly where interstate commerce is involved. Because of this fragmentation, activities lawful in one state may be prohibited in another.

Skill-Based Games

Some Mini Apps may involve games that are primarily skill-based. While these may fall outside gambling regulation in certain jurisdictions, this is not guaranteed. Regulators may still scrutinise:

- Whether any element of chance influences the outcome.
- Whether users pay to participate.
- Whether prizes have real-world or transferable value.

Competitive games, tournaments, or esports-style features offering cash, crypto, or valuable digital items as rewards may still be regulated or restricted in some jurisdictions.

Loot Boxes and Randomised Rewards

Loot boxes and similar mechanics are increasingly scrutinised by regulators, particularly where:

- Users pay to access randomised rewards.
- Rewards have monetary value or can be transferred, sold, or exchanged.
- The mechanic resembles gambling in substance.

Some jurisdictions treat loot boxes as a form of gambling, while others regulate them under consumer protection or youth protection laws. Disclosure of odds, spending limits, and restrictions on minors may be required.

Regulated Activity

If there is no intention to operate a licensed gambling business, the Mini App must be structured so that it does not meet the legal definition of gambling in the jurisdictions where it is accessible. This may involve:

- Removing payment or staking requirements.
- Eliminating or materially reducing elements of chance.
- Ensuring prizes have no monetary or transferable value.
- Preventing secondary markets or redemption mechanisms.
- Clearly framing activities as entertainment rather than profit-oriented.

Design and monetisation choices are often critical in determining whether an activity is regulated.

If the developer intends to operate gaming or gambling services directly through the Mini App, formal licensing is typically required before launch. Licensing regimes often involve:

- Establishing a licensed entity in the relevant jurisdiction(s).
- Meeting capital, integrity, and organisational requirements.
- Implementing age verification, responsible gaming, and player protection measures.
- Ensuring fairness, transparency, and auditability of game mechanics.
- Submitting to ongoing regulatory supervision, reporting, and audits.

Licensing processes are often time-consuming and may impose strict limitations on marketing, user onboarding, and permitted jurisdictions.

Licensing and Authorisation Requirements

Where a Mini App carries out a regulated activity, the developer must obtain the relevant licence or authorisation before launch. Operating without authorisation may result in enforcement action, fines or service restrictions.

Authorisation regimes typically require:

- Establishing an appropriate legal entity with genuine local presence.
- Meeting financial, capital and safeguarding requirements.
- Appointing fit and proper directors and compliance personnel.
- Implementing robust internal policies, including AML, risk management, data protection and cybersecurity.
- Complying with ongoing reporting, audit and supervisory obligations.

Developers should monitor regulatory developments and ensure regulated services are not offered in jurisdictions where authorisation has not been obtained.

2.3 World App Rules

> *"World App has its own set of rules that Mini Apps must follow, in addition to applicable laws and marketplace policies."*

Overview

World App has its own set of rules that Mini Apps must follow, in addition to applicable laws and marketplace policies. This section covers the legally relevant World App rules only — for technical, UX, and visual requirements, refer to the official World App documentation.[14] These rules may change over time; therefore, always check the latest version.

Branding and Naming

Do not use the words "World", "official" or the World App's logo in your app's name or interface. Names must be simple and distinctive. Mini Apps must not impersonate TFH (operator of the World App) or Worldcoin in any way – this can constitute misleading advertising or consumer fraud and may mislead users into believing the Mini App is official or endorsed.

Do not mimic other apps or brands; avoid terms that resemble third-party registered trademarks, explicit content, generic functional names (such as "Earn", "Swap"), special characters or emojis, and ensure the name is appropriate across major languages.

Gaming and Gambling

Games can generally be divided into skill-based (where the user's ability meaningfully affects the outcome, such as puzzle or strategy games) and chance-based categories (where the outcome is determined predominantly by randomness, such as roulette-style mechanics, lotteries, or randomised prize boxes). Sports betting is generally treated as chance-based, even where the user follows teams or statistics.

Chance-based mechanics may constitute gambling in many jurisdictions, and offering them without a valid gambling licence may be unlawful. App Store and Google Play also require that any gambling-related apps hold all necessary licences and operate only in jurisdictions where those licences are valid.

Paid Memberships and Increased Yield

Mini Apps must not offer memberships, subscriptions or paid tiers that grant users higher yield, returns or enhanced earning rates. These models create tiered financial returns dependent on payment and potentially new user inflows, which may resemble Ponzi-like schemes that are prohibited in many jurisdictions.

Token Presales

Mini Apps must not conduct, advertise or facilitate token presales. Token presales are restricted because they often resemble unregistered investment offerings, may trigger securities regulation in multiple jurisdictions, and present high consumer protection risks. Many scams also disguise themselves as presales, which is why platforms prohibit them as a protective measure.

However, having a token is not prohibited for a Mini App. A token may function as a utility token with certain features inside the app.

Developers must also note that native tokens cannot be used as a payment method within the Mini App at this stage. For more detail on permitted and prohibited payment mechanisms, consult the "Payments" section of these guidelines.

Prohibited Content

Mini Apps must not include any of the following: defamatory, discriminatory or hateful material; realistic violence or encouragement of violence; facilitation of weapon sales; overtly sexual or pornographic content; NSFW (Not Safe For Work) content of any kind; misleading or false information; harmful content exploiting crises; impersonation of TFH (World App operator) or Worldcoin.

If a Mini App allows users to publish content, the developer must implement effective moderation. Users have the right to be protected from harmful or unlawful content even where such content is published by other users rather than by the Mini App operator.

Smart Contract Considerations

You can deploy either immutable smart contracts or those which are upgradeable. In the latter case it must:

- Use a multi-signature upgrade authorisation where the World App operator holds 1 of 2 keys.
- Require the World App operator's review and written approval before any upgrade is executed.
- Be subject to a public notice period (recommended: 48–72 hours) before upgrade execution.

Upgradeability on the World App platform is limited: it should be used only for restricted parameters, such as protocol fees, rather than to alter the fundamental behaviour of the contract.

Smart contract code and relevant documentation shall be made available at least to the reviewers.

Violations of the above rules may result in consequences such as rejection of the Mini App during the review process or removal from the platform after publication.

3. Operating Requirements

3.1 Corporate Structure

While some developers may initially build or test a Mini App as individuals, developers intending to distribute or operate a Mini App long-term should strongly consider operating through a legal entity rather than as an individual. The choice of corporate structure has direct implications for personal liability, taxation, intellectual property ownership, funding, and regulatory compliance.

> *"Developers intending to distribute or operate a Mini App long-term should strongly consider operating through a legal entity rather than as an individual."*

Liability Protection

Where a Mini App is operated by an individual, the developer may be personally liable for user claims, regulatory fines, data protection breaches, and contractual obligations. Operating through a properly formed legal entity (such as a limited company) generally limits liability to the assets of that entity, subject to applicable law and compliance with corporate formalities.

Funding and Commercial Relationships

Most third parties expect to deal with a legal entity. A corporate structure is typically essential to raise funding,

enter into commercial contracts, integrate with payment processors or app distribution platforms, and appoint employees or contractors. Many service providers will not contract with individuals at all, particularly where regulated or financial services are involved.

Tax Planning

A corporate structure enables more structured tax treatment, including clear separation between personal and business income, deduction of legitimate business expenses, structured handling of VAT and indirect taxes, and improved management of cross-border taxation.

Intellectual Property Ownership

A legal entity provides a clear framework for owning and managing intellectual property associated with the Mini App, including source code and software, trademarks, branding, domain names, designs, databases, and proprietary content.

Where development is conducted by multiple contributors, or where contractors are involved, a corporate structure helps ensure that IP rights are properly assigned and consolidated in a single owner. This is particularly important for future fundraising, licensing, or exit transactions.

Regulatory Considerations

Many regulated activities, such as payment services, crypto asset services, securities-related activities, or gambling, cannot legally be conducted by individuals and require a licensed legal entity.

Regulators often expect a clearly identifiable operating entity, responsible persons and management oversight, and documented policies and procedures. Operating through a legal entity can therefore be a practical prerequisite for regulatory compliance.

Individual Development

In limited circumstances, a Mini App may be developed and operated by an individual — for example, experimental or proof-of-concept apps, non-commercial or open-source projects, educational apps with no monetisation, or internal tools. Even in these cases, personal liability still applies, consumer protection and data protection laws may be relevant, and monetisation or scaling may quickly necessitate incorporation.

Many developers begin as individuals and later incorporate as their Mini App matures. Developers transitioning to a corporate structure should plan for the transfer of intellectual property, migration of contracts and user-facing terms, updates to legal documentation, and tax considerations associated with the transfer of assets or income.

Choosing an Appropriate Entity and Jurisdiction

Selecting the right jurisdiction and corporate structure is a strategic decision that affects liability, taxation, funding, governance, and regulatory compliance. There is no one-size-fits-all approach; the appropriate structure depends on the nature and scale of the Mini App.

When choosing a jurisdiction, developers typically consider:

- legal and regulatory environment;
- location of founders, team, and users;
- availability of banking and payment services;
- tax framework;
- investor acceptance and reputation.

Common entity types include limited liability companies (widely used for tech projects due to flexibility and investor acceptance), corporations (often preferred where institutional or venture capital investment is anticipated), partnerships (generally less suitable due to liability and scalability limitations), and foundations or similar structures (sometimes used for ecosystem-driven or open-source projects alongside separate operating entities). The choice of entity should align with the intended business model and regulatory exposure.

Corporate structure also depends on the number of founders and team members. Multi-founder or growing teams generally require clearer rules on decision-making, equity allocation, and control, as well as the ability to employ staff and issue incentives.

Expected funding sources often shape both jurisdiction and entity choice. Venture capital and institutional investors commonly prefer familiar jurisdictions and entity forms, while more complex funding models may require separation between operational and ownership structures.

Developers should also consider whether the entity is treated as a pass-through structure or taxable at the corporate level, along with withholding taxes, indirect taxes, and cross-border tax exposure.

As projects scale or become regulated, more sophisticated structures may be appropriate, such as holding companies, operating subsidiaries, or special purpose vehicles (SPVs) for specific markets or regulated activities.

3.2 Terms & Conditions

Every Mini App must have its own user-facing Terms & Conditions and Privacy Policy. This is a mandatory requirement imposed by the World App (point 2.4 of TFH Developer Portal Terms[15]).

> *"Every Mini App must have its own user-facing Terms & Conditions and Privacy Policy."*

T&Cs establish the legal relationship between the Mini App operator and its users. T&Cs act as an agreement: they define rights and responsibilities, allocate risk, determine dispute mechanisms and limit liability. Properly drafted T&Cs can reduce legal exposure.

Core provisions typically include:

- Limitations of liability.
- Prohibited uses, specifying what users are not allowed to do inside the Mini App.
- Content rules, including requirements for user-generated content and the Mini App's right to moderate or remove harmful material.
- Dispute resolution mechanisms.
- Applicable law.

Why Terms & Conditions Matter

T&Cs are not a formality. They operate as a legal safeguard. Without them, default consumer protection rules may apply, often to the developer's disadvantage.

For example, in jurisdictions permitting collective actions, the absence of protective clauses may expose a developer to significant collective litigation. In some cases, well drafted T&Cs may determine whether a claim would be brought at all.

Enforceability: Why Format and Implementation Matter

Having T&Cs is insufficient unless they are enforceable. Enforceability is a legal concept that determines whether T&C or other legal agreements can be upheld in court in the event of a dispute. If a provision is enforceable, the jurisdiction's legal system can compel the violating party to comply. If unenforceable, they cannot be relied upon in a dispute.

Enforceability may fail for several reasons:

- Unfair or invalid clauses.
- Failure to obtain proper user consent.
- Formatting issues, such as hiding important clauses in small fonts.

Common Mistakes to Avoid

- Poor drafting. AI tools without professional review cannot fully capture the specific features, regulatory considerations and risks of a particular Mini App. Such documents often contain invalid clauses or omit essential provisions.
- Copying another project's T&Cs. T&Cs are protected by copyright, and copying them is both unlawful and reputationally damaging. More importantly, another project's terms will not reflect your business model, jurisdictions, payment flows, or regulatory exposure. Copying also replicates any legal mistakes the original text may contain.
- Unfair terms. Consumer protection laws prohibit terms that unreasonably disadvantage users. Unfair terms will be deemed non-binding for consumers in case of a dispute.

Checklist for Well-Prepared T&Cs

- T&C were drafted by professionals with a deep understanding of your specific product or service, its features and functionality, as well as applicable regulations.
- T&C contain no unfair provisions.
- T&C are designed for your specific project.
- T&C include all necessary information required to form a valid contract under the applicable law.
- The technical and UI implementation ensures that the customers' consent is obtained properly and in accordance with legal requirements, and that the customers can easily access their full text.

3.3 Taxation

Tax requirements apply regardless of whether a Mini App operates in a regulated sector and may arise even where revenue is modest or generated across borders. Revenue generated through a Mini App — such as fees, subscriptions, advertising income, commissions, or in-app purchases — is generally subject to taxation, and developers may be required to report income, pay income or corporate taxes, and maintain appropriate accounting records. Tax obligations may arise in more than one jurisdiction, depending on where the developer is established, where users are located, and how revenue is generated.

> *"Operating through a company can provide more predictable tax treatment as the Mini App scales."*

Individuals operating Mini App are typically taxed on Mini App income as personal income at progressive rates. Companies are generally taxed at corporate rates with clearer separation between business and personal income. Operating through a company can provide more predictable tax treatment as the Mini App scales.

In many jurisdictions, indirect taxes such as VAT, GST, or sales tax may apply to supplies made through a Mini App, particularly for digital services or digital content. VAT/GST rules vary significantly by jurisdiction and are often complex for cross-border digital services. Developers may need to register for VAT/GST in relevant jurisdictions, charge the appropriate tax rate based on user location, collect and remit taxes to tax authorities, and maintain transaction-level records.

4. Payments

Mini Apps may accept payments in two forms: supported crypto assets and fiat. Developers bear full responsibility for managing payments, handling disputes, processing refunds, and complying with all applicable payments and consumer protection laws.

4.1 Crypto Assets

At present, only $USDC and $WLD are supported for payments within World App. These transactions rely on users' self-custodial wallets, meaning:

- The World App does not store, custody, transmit, or control crypto assets at any point;
- All token transfers occur on the relevant blockchain; and
- World App cannot assist with failed or incorrect transactions, as it is not a party to them.

A transaction in crypto assets in a Mini App takes place only between the user's non-custodial wallet and the developer's wallet.

4.2 Fiat Payments

Where supported, Mini Apps may integrate Apple Pay or Google Pay for fiat transactions.

Unlike crypto-asset payments, fiat payments may be subject to chargebacks, meaning the user can dispute a transaction directly with their bank or payment provider and the payment may be reversed without the developer's consent or involvement. Chargebacks may occur, for example, where the user claims an unauthorised transaction, payment processing errors, or incorrect charges.

Developers cannot control or prevent chargebacks initiated through payment providers. If a chargeback is approved:

- The developer loses the payment; and
- The user may retain access to the purchased service or product (depending on the nature of those).

Developers should therefore assess the risks of accepting fiat payments for non-revocable goods or services, such as irreversible digital items or one-time access rights.

Refund rules and consumer rights are described separately in the "Refunds" section below.

5. Privacy and Data Protection

Mini Apps often collect, use, and process user data. Developers must consider applicable privacy and data protection laws from the outset – regardless of whether

the Mini App operates in a regulated industry or generates revenue.

5.1 Data Protection Regimes

Data protection obligations depend on where the operating company is incorporated, where users are located, and how personal data is processed. Key regimes include:

- European Union: the General Data Protection Regulation (GDPR), which applies broadly to the processing of personal data of individuals in the EU, regardless of where the developer is established.
- United States: state-level privacy laws such as the California Consumer Privacy Act (CCPA) and similar statutes in other states.
- Other jurisdictions: many countries have adopted comprehensive data protection laws (e.g. the UK GDPR, Brazil's LGPD, Singapore's PDPA), which may apply based on user location or business activity.

Developers should assume that privacy laws may apply cross-border and may impose obligations even where no local presence exists.

5.2 Personal Data

Personal data generally includes any information relating to an identified or identifiable individual. Depending on the applicable regime, this may include:

- Direct identifiers, such as names, usernames, email addresses, phone numbers, or account details.
- Online or technical identifiers, including IP addresses, device identifiers, cookies, and similar tracking technologies.
- Usage, behavioural, or interaction data that can be linked to a specific user or account.
- Location data, transaction data, or communications metadata.

Certain categories of data may be subject to enhanced protection requirements under applicable laws, including sensitive data (such as payment information, health data, or biometric data) and data relating to minors.

5.3 High-Level Obligations in Relation to Personal Data

Although specific requirements vary by jurisdiction, data protection regimes generally require developers to:

- Have a lawful basis or justification for collecting and processing personal data.
- Use personal data in a manner that is consistent with applicable legal requirements and disclosed purposes.
- Implement appropriate safeguards and governance measures to ensure compliant handling of personal data throughout its lifecycle.

5.4 Transparency and User Notices

Data protection regimes typically require developers to provide clear and accessible information to users about how their data is processed. Notices should be easy to understand and available before or at the point of data collection. This typically includes:

> *"Data protection regimes typically require developers to provide clear and accessible information to users about how their data is processed."*

- A privacy notice explaining what data is collected, how it is used, and with whom it is shared.
- Disclosure of any tracking, analytics, or profiling activities.
- Information about user rights (such as access, deletion, or objection).

5.5 Data Minimisation, Security, and Retention

Developers are generally expected to follow core data protection principles, including:

- Data minimisation: collecting only the data necessary for the intended purpose.
- Security: implementing appropriate technical and organisational measures to protect data against unauthorised access, loss, or misuse, such as access controls, encryption, and incident response planning.
- Retention limitation: retaining personal data only for as long as necessary and deleting or anonymising it when no longer required.

5.6 SDKs, Analytics, Cookies, and Third-Party Integrations

Mini Apps often rely on third-party SDKs, analytics tools, or external services. Developers remain responsible for data protection compliance even where data is processed by third parties. Integrating third-party tools without proper oversight may expose developers to compliance risks, even if the data is processed off-platform. Therefore, developers should:

> *"Developers remain responsible for data protection compliance even where data is processed by third parties."*

- Understand what data third-party tools collect and how it is used.
- Ensure appropriate contractual arrangements are in place with third-party providers.
- Disclose third-party data sharing in privacy notices.
- Obtain user consent where required, particularly for tracking, analytics, or marketing cookies.
- Limit third-party access to data to what is strictly necessary.

6. Consumer Protection

6.1 General

Consumer protection laws may apply to the operation of Mini Apps, particularly where users interact with the service in a non-professional capacity. These laws impose mandatory rules that take precedence over the terms of any user agreement. This means that Mini Apps Terms & Conditions cannot limit or remove rights granted to consumers under applicable law.

> *"Developers must ensure that all interactions with users are transparent, fair and non-misleading."*

Specific requirements vary by jurisdiction, but the following general obligations commonly apply:

- Accuracy and transparency: All fees, prices and currencies must be clearly displayed before payment.
- Access to documents: Users must be able to review the Terms & Conditions and Privacy Policy before completing a transaction, and these must remain accessible at all times.
- Fair terms: Consumer protection laws require contract terms to be fair. Provisions that place consumers at an unreasonable disadvantage may be unenforceable.
- Honest communication: Developers must not use misleading statements, pressure tactics or ambiguous wording. Descriptions of features and limitations must be accurate and complete.
- Dispute resolution: Developers must implement fair and transparent complaint and dispute handling processes.

In essence, developers must ensure that all interactions with users are transparent, fair and non-misleading.

In practice, compliance with consumer protection legislation includes:

- Legal documentation, such Terms & Conditions, Refund Policy, Privacy Policy.
- Product structure and mechanics, including how pricing, functionality, and delivery are designed.
- UI and user flows, i.e., how information is presented and whether it is prominent and understandable.
- Marketing and promotion, such as how features, pricing, discounts, and benefits are communicated to users.

For example, fee disclosures must be clear and meaningful. It may not be sufficient to disclose additional fees or commissions if they are hidden in fine print or only presented at the final stage of checkout. Likewise, Terms & Conditions must comply with consumer protection laws and must not, for example, exclude mandatory refund rights or impose unfair limitations of liability on consumers where such protections apply.

6.2 Refunds

Refund rights typically arise from two sources: statutory cancellation rights for distance contracts and remedies

for goods or services that are not of satisfactory quality. While rules vary by jurisdiction, the following principles are common.

Cancellation Rights in Distance Contracts

In many jurisdictions, consumers have a statutory right to cancel certain contracts concluded at a distance, including online purchases. In practice, this often means that:

- There is a mandatory minimal cancellation period.
- The cancellation period usually begins when the contract is concluded.
- The consumer may withdraw without giving any reason.
- The consumer should not incur liability for cancellation.
- This right applies regardless of whether payment was made in fiat or crypto assets.

There is an essential exception for digital products or services that are made available immediately after purchase, in which case cancellation rights may not apply.

However, developers may choose to grant cancellation rights that are broader than those required by law, such as offering a longer cancellation period longer than required under the law. Similarly, where consumer protection legislation does not mandate cancellation rights, developers may still provide them contractually through explicit agreement with users.

Non-Satisfactory Quality of Goods or Services

Separate from cancellation rights, consumer protection laws typically require that goods and services meet a minimum standard of quality. Non-satisfactory quality may include situations where a product or service:

- Is not as described.
- Is defective or faulty.
- Is not fit for its intended purpose.
- Does not meet reasonable quality expectations.
- Is not delivered within the agreed timeframe.

Where goods or services are of non-satisfactory quality, consumers are generally entitled to legal remedies, which may include repair, replacement, price reduction, or a refund.

6.3 Unfair Commercial Practices

Mini Apps must not engage in unfair commercial practices – meaning practices that mislead consumers, use aggressive tactics, or otherwise treat consumers unfairly.[16]

> *"Mini Apps must not engage in unfair commercial practices – meaning practices that mislead consumers, use aggressive tactics, or otherwise treat consumers unfairly."*

Misleading Actions and Omissions

It is prohibited to make false, inaccurate or ambiguous statements about a product or service. This includes presenting an offer as "limited" or "exclusive" where no such limit exists, overstating benefits, or omitting material information necessary for an informed decision.

Omission includes failing to provide information or presenting it in a way that is unclear, delayed or unlikely to be noticed. Developers must therefore ensure that key information is displayed prominently, taking into account font size, placement, colour and user flow.

False or Unrealistic Statements

Mini Apps must not make claims that cannot be substantiated. Statements guaranteeing financial returns, promising unachievable outcomes or misrepresenting risk levels are likely to be materially misleading.

Drip Pricing

"Drip pricing" arises where an initial price is presented but additional charges are added during the checkout process. All prices, fees and payment terms must be clearly disclosed before the user confirms the transaction.

Although disclosure requirements vary by jurisdiction, developers should clearly and prominently provide:

- The main characteristics of the product or service.
- The total price payable, including the currency, and how the price is calculated if it cannot be fixed in advance.
- Any additional charges the user may incur (such as taxes, delivery fees, or platform fees).

- Identity of the developer or operating entity.
- Whether the user has any statutory right to cancel the contract.
- Any other conditions that materially affect the user's decision to purchase (for example, usage limitations, access duration, or restrictions on refunds).

Such information must not be hidden in small print or disclosed only at the final checkout stage. It should be clear and sufficiently prominent for an average user.

Examples

The following are typical examples of unfair commercial practices that developers should avoid:

- Advertising a bonus, discount or "limited time offer" that does not actually exist.
- Omitting key details about fees, risks or requirements until after the user has made a purchase.
- Misrepresenting the nature or function of a feature (e.g., implying guaranteed returns when in practice they are not guaranteed).
- Concealing payment terms, additional charges, taxes, or delivery fees until after checkout.
- Applying undue pressure in promotional messaging or onboarding to induce a user to transact.

7. Intellectual Property Basics

7.1 Why Intellectual Property Matters for Mini Apps

Intellectual property (IP) is a key asset of any Mini App. It includes source code, the Mini App's name, logo, visual identity, content, and other materials used to deliver the product.

> *"The fact that IP and materials exist does not automatically mean that a developer or project owns or has the right to use it."*

Importantly, the fact that IP and materials exist does not automatically mean that a developer or project owns or has the right to use it. Mini App teams should address two core IP questions:

- Ownership of IP rights (for example, code and design created by the team or contractors should be assigned to the project; otherwise, the team or contractors may remain the IP owners and could potentially prohibit or restrict its use).
- Right to use third-party materials (for example, you should ensure that third-party code, fonts, images, branding elements, or other materials are permitted to use).

7.2 Copyright: Code and Content

Copyright is the most common form of IP protection. Under international treaties and most national laws, copyright protects software code, written content, imagery, graphics, video, audio, animations and user interface elements. Copyright protection arises automatically when a work is created – no registration is required.

Code: Copyright Protection and Limitations

Software code is generally protected by copyright as a literary work. This protection covers the expression of the code, meaning the specific way in which the code is written.

However, it should be noted that copyright does not protect ideas or concepts, algorithms as such, and methods of operation. For example, while a specific implementation of an algorithm may be protected, the underlying logic or functionality may not be.

In addition to copyright, some aspects of a Mini App (such as proprietary algorithms or internal processes) may be protected as trade secrets, provided they are kept confidential and reasonable measures are taken to preserve secrecy.

7.3 Trademarks and Brand Assets

Trademarks protect names, logos and other identifiers that distinguish products or services. Unlike copyright, trademark protection is jurisdiction-specific and typically requires registration in each country or region where protection is sought.

> *"Developers should conduct trademark searches before selecting a name, focusing on the key jurisdictions where the Mini App will operate."*

Trademarks and Naming

A trademark may be registered and protected for certain goods or services in one jurisdiction but not in others. If a particular mark is not registered for the relevant goods or services in a given jurisdiction, it may be possible to use that name locally. However, doing so may prevent the Mini App from being lawfully offered in jurisdictions where the trademark is registered. Well-known trademarks may also be protected even without local registration.

Developers should conduct trademark searches before selecting a name, focusing on the key jurisdictions where the Mini App will operate.

Brand Assets and Visual Identity

Logos and distinctive visual elements often benefit from overlapping protection:

- Trademark law protects them as identifiers of commercial origin; and
- Copyright law protects their creative expression.

The main distinction is that copyright protection is automatic, while trademark protection generally applies from the moment of registration. Trademarks are usually required once a brand becomes well known and there is a high likelihood of infringement.

7.4 Third-Party Code

Public availability of source code does not, in itself, grant any right of use. In the absence of a valid licence, all IP rights remain reserved by the original rights holder.

> *"Public availability of source code does not, in itself, grant any right of use. In the absence of a valid licence, all IP rights remain reserved by the original rights holder."*

In practice, third-party code may be:

- Distributed under an open-source licence. Common open-source licence categories include:
- Permissive licences (e.g. MIT, Apache 2.0), which allow reuse with minimal obligations, usually requiring attribution; and
- Copyleft licences (e.g. GPLv3), which impose conditions on redistribution and may require derivative works to be released under the same licence.
- Distributed under a commercial or custom licence.
- Published without any licence at all.

Where no licence is mentioned, the code cannot be used. Where a licence does apply, including an open source licence, use is permitted only in accordance with its terms. Developers should ensure that the licence conditions are compatible with the intended use and distribution model.

7.5 User-Generated Content

If a Mini App allows users to upload or publish content, developers should treat that content as user-owned IP. Hosting content inside the Mini App does not make it the developer's property.

Developers should obtain an appropriate licence from users – one that permits the developer to host, display and reproduce user-generated content as necessary to operate the Mini App. The licence should also expressly reserve the right to moderate and remove content in accordance with the Mini App's rules and applicable law.

7.6 Ownership and Assignment of IP

IP rights generally belong to the individual who creates the work – they do not automatically vest in the project or entity behind the Mini App without an agreement.

> *"IP ownership does not transfer by default and should be clearly addressed in the contract."*

The allocation of IP rights depends on the legal relationship with the person who created the work:

- Employees: IP created in the course of employment will generally belong to the employer, subject to applicable local law and the terms of the employment

agreement.

- Independent contractors: IP ownership does not transfer by default and should be clearly addressed in the contract.

8. Q&A

Do I need a legal entity to launch a Mini App?	Not strictly required, but strongly recommended if you plan to monetise, scale, or enter into commercial relationships. Operating as an individual exposes you to unlimited personal liability. A legal entity (such as a limited liability company) separates personal and business risk, enables you to raise funding, contract with payment providers, and manage taxes more effectively. See “Corporate Structure” section.
Can my Mini App accept crypto payments?	Yes. At present, only $USDC and $WLD are supported for payments within World App. These transactions rely on users’ self-custodial wallets, meaning the World App does not store, custody, or control crypto assets at any point. All token transfers occur on the relevant blockchain. The developer bears full responsibility for managing payments, handling disputes, addressing failed transactions, and complying with applicable laws. See “Payments” section.
Does my Mini App need Terms & Conditions?	Yes. Every Mini App that offers goods, services, or digital content to users should have clearly drafted Terms & Conditions. T&Cs define the legal relationship between the developer and the user, allocate risk, and establish the rules governing transactions, refunds, liability, and dispute resolution. Poorly drafted or missing T&Cs can leave the developer exposed to regulatory action, unenforceable claims, and class-action liability. See “Terms & Conditions” section.
My Mini App includes a game with prizes. Is that gambling?	It depends on whether the outcome is determined primarily by skill or by chance. Skill-based games (where the user’s ability meaningfully affects the outcome, such as puzzle or strategy games) are generally not classified as gambling. Chance-based games (where the outcome is determined predominantly by randomness, such as roulette-style mechanics, lotteries, or randomised prize boxes) may constitute gambling in many jurisdictions. Offering chance-based mechanics without a valid gambling licence may be unlawful. App Store and Google Play also require that gambling-related apps hold all necessary licences. See “Gaming and Gambling” and “Gaming and Gambling Regulation” sections.

Could my Mini App token be classified as a security?	Potentially, yes. If a token grants holders economic rights (such as revenue sharing, profit participation, or governance over treasury funds), or if it is marketed as an investment opportunity, it may be classified as a security under the laws of many jurisdictions. Securities are subject to strict regulatory requirements including registration, disclosure obligations, and licensing. Tokens that function purely as utility tokens (granting access to a service or feature) are less likely to be classified as securities, but the distinction depends on the specific facts and applicable law. See “Securities and Investment Services Regulation” section.
What privacy laws apply to my Mini App?	It depends on where your company is incorporated, where your users are located, and how you process personal data. Key regimes include the EU GDPR (applicable to any processing of personal data of individuals in the EU, regardless of where the developer is based), US state-level privacy laws such as the CCPA, and comprehensive data protection frameworks in other jurisdictions such as Brazil’s LGPD, Singapore’s PDPA, and the UK GDPR. Developers should assume that privacy laws may apply cross-border and may impose obligations even without a local presence. See “Privacy and Data Protection” section.
Do I need to offer refunds?	In many jurisdictions, consumers have a statutory right to cancel distance contracts (including online purchases) within a mandatory cancellation period, without giving a reason. This right applies regardless of whether payment was made in fiat or crypto. An important exception exists for digital products or services made available immediately after purchase – in such cases, cancellation rights may not apply. In addition, where a product or service does not meet the quality standards reasonably expected by the consumer, the consumer may be entitled to a refund, replacement, or repair. These rights exist independently of any voluntary refund policy the developer may offer. See “Consumer Protection” section.
What are the rules for upgradeable smart contracts?	If your Mini App deploys upgradeable smart contracts, you must use multi-signature upgrade authorisation where Tools For Humanity (TFH) holds one of two keys, require TFH review and written approval before any upgrade is executed, and implement a public notice period (recommended: 48–72 hours) before the upgrade goes live. Upgradeability should be limited to restricted parameters such as protocol fees – it must not be used to alter the fundamental behaviour of the contract. Smart contract code and relevant documentation must be made available to reviewers. See “Smart Contract Consideration” section.

Do I need to pay tax on Mini App revenue?	Yes. Mini App developers are generally subject to taxation in the jurisdictions where they are resident or incorporated, and may also have obligations in jurisdictions where their users are located. Operating through a legal entity enables structured tax treatment, including separation of personal and business income, deduction of legitimate business expenses, and management of cross-border taxation. VAT or GST obligations may also apply, particularly where digital services are sold to consumers in jurisdictions that impose indirect taxes on such transactions. See “Tax Planning” and “Taxation” sections.
I use third-party SDKs and analytics. Am I responsible for how they handle data?	Yes. Developers remain responsible for data protection compliance even where data is processed by third parties. Integrating third-party tools without proper oversight may expose you to compliance risks, even if the data is processed off-platform. You should understand what data each tool collects and how it is used, put appropriate contractual arrangements in place with providers, disclose third-party data sharing in your privacy notice, obtain user consent where required (particularly for tracking and marketing cookies), and limit third-party access to what is strictly necessary. See “SDKs, Analytics, Cookies, and Third-Party Integrations” section.
Who owns the IP in my Mini App if I hired freelance developers?	The freelance developer does, by default. Intellectual property rights generally belong to the individual who creates the work. For independent contractors, IP ownership does not transfer automatically – it must be expressly assigned in the contract, typically through an assignment of IP rights to the entity operating the Mini App, or at a minimum, a broad and irrevocable licence permitting use of the work. If you are using a legal entity, IP should be assigned to the entity, not to you personally. See “Ownership and Assignment of IP” section.
Can I use open-source code in my Mini App?	Yes, but only in accordance with the applicable licence terms. Open-source licences fall into two broad categories: permissive licences (e.g. MIT, Apache 2.0), which allow reuse with minimal obligations such as attribution, and copyleft licences (e.g. GPLv3), which impose conditions on redistribution and may require derivative works to be released under the same licence. Code published without any licence cannot be used – public availability does not grant a right of use. Developers should maintain a record of all third-party code used, along with applicable licence terms and compliance obligations. See “Third-Party Code” section.
What happens if my Mini App is found to be non-compliant?	Non-compliance can result in rejection during the World App review process, removal from the platform after publication, regulatory enforcement action (including fines and sanctions) from relevant authorities, civil claims from users, and reputational damage. The specific consequences depend on the nature and severity of the non-compliance and the applicable jurisdiction.

References

[1] https://whitepaper.world.org/

[2] https://world.org/

[3] https://developer.apple.com/app-store/review/guidelines/

[4] https://support.google.com/googleplay/android-developer/answer/9859455?hl=en

[5] https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng

[6] https://www.legislation.gov.uk/uksi/2011/99/contents

[7] https://www.legislation.gov.uk/uksi/2017/752/contents

[8] https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng

[9] https://www.legislation.gov.uk/ukpga/2000/8/contents

[10] https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf

[11] https://www.govinfo.gov/content/pkg/COMPS-1885/pdf/COMPS-1885.pdf

[12] https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

[13] https://www.legislation.gov.uk/uksi/2017/692/contents/made

[14] https://docs.world.org/mini-apps

[15] https://worldcoin.pactsafe.io/rjd5nsvyq.html#contract-b1q9midy9

[16] https://assets.publishing.service.gov.uk/media/691b9bd821ef5aaa6543ee6f/Unfair_commercial_practices_CMA207_18_Nov_2025__2_.pdf

Contributors

Pavel Batishchev
Managing Partner
batishchev@aurum.law

Illia Shenheliia
Associate Partner
shenheliia@aurum.law

Valeriia Sych
Junior Associate
sych@aurum.law

Disclaimer

This guide is for informational purposes only and does not constitute legal advice. For guidance specific to your project, consult a qualified professional.

The information contained in this document is provided ‘as is’ without warranty of any kind. AURUM disclaims all liability for actions taken or not taken based on the content of this guide.

Since 2011, Aurum has supported founders, projects, and investors building the digital economy, focusing on next-gen tech, blockchain, alternative finance, and frontier innovation.

/AURUM

Legal partner behind the builders of tomorrow ©