CUSTOMER ONBOARDING GUIDE

veriff

How to get more high-value customers using your platform

Introduction

Acquiring and onboarding new customers goes beyond a simple registration form—it's one of the first meaningful interactions they have with your product, shaping expectations for the entire relationship.

A well-designed onboarding experience can dramatically increase user activation and retention, whereas a poor experience leads to drop-offs and lost business.

In industries that require customer identity verification (IDV) and Know Your Customer (KYC) compliance, the onboarding process becomes even more complex.

Organizations that offer streamlined **digital onboarding** have seen customer acquisition rates increase by **50–60%** compared to traditional (in-person or paper-based) processes (Source: Hubspot)

In the financial sector, cumbersome onboarding has driven abandonment rates as high as 68% in recent years, representing billions in lost revenue (Source: Veriff KYC guide).

This guide explores best practices and strategies for designing an onboarding flow that reduces friction, boosts conversions, and ensures regulatory compliance.

Contents

1/

How to build a high-converting customer onboarding process with identity verification

Many businesses overlook the importance of a thoughtful customer onboarding strategy. Moreover, a one-size-fits-all approach rarely delivers the best results. Here's how you can build a customer onboarding strategy that works for your business.

Understanding your business and audience

Start by tailoring the onboarding and Identity verification process to your specific context and users. Identify what level of verification is truly needed for your service (based on industry regulations and fraud risk) and what your typical user is like (tech-savvy, demographics, etc.).

For example, if only a small portion of your users are high-risk, **consider a risk-based approach:** McKinsey estimates fewer than 5% of new bank customers are high-risk, so imposing heavy checks on **every user** isn't necessary and it might only be necessary to implement more stringent checks at a later stage in their customer journey - such as when they want to make their first payment or a transfer over a certain value.

By segmenting users based on risk, you can apply enhanced verification and stricter requests only where it's truly needed. This aligns onboarding with business objectives – you stay compliant by thoroughly vetting risky users, but **streamline the process for the 95% low-risk majority** to keep conversion high.

Another aspect to consider is your audience's needs: tech-savvy users might expect a **mobile-first experience**, so ensure your verification flow works smoothly on smartphones and tablets (Source: Gainsight).

If your user base spans multiple countries, choose IDV methods that cover various document types and languages (for instance, Legitfy, a cross-border notarization solution, had to verify IDs from several European countries).

Understanding both your business requirements and user expectations will inform an onboarding design that balances security with convenience.

Aligning onboarding with sector and go-to-market strategy

Your onboarding strategy should directly support your product's goals – whether that's rapid user growth, trusted security, or global expansion.

Define clear objectives (e.g. maximize completed sign-ups, minimize fraud, ensure compliance in X markets) and let these guide your design decisions.

Match onboarding strategy with go-to-market approach

Align your onboarding type clearly with your go-to-market strategy:

Product-Led	→	Fully automated, self-serve user sign-up and onboarding.	EXAMPLE: **Typeform**
Product-Led Success-Assisted	→	Self-serve product onboarding supported by onboarding specialists.	EXAMPLE: SUPERHUMAN
Product-Led Sales-Assisted	→	Customization, volume discounts or specific feature access granted only after interaction with sales.	EXAMPLE: ATLASSIAN
Sales-Led	→	Full enterprise-level sales team intervention required before onboarding.	EXAMPLE: salesforce

For instance, if the goal is to grow your user base quickly, you might allow users to start using the product with minimal information and only prompt full KYC when necessary (this is sometimes called **progressive onboarding** or tiered verification).

On the other hand, if your business objective is to establish a reputation for security and compliance (common in fintech or crypto), you'll want to communicate that upfront and ensure the verification process (while seamless) leaves no compliance gaps.

Always weigh the trade-offs.

More friction can mean fewer sign-ups, but too little verification can mean compliance risks – so find a sweet spot that meets **regulatory needs and business KPIs.**

Reducing friction during sign-up typically **boosts conversion rates**—but if not enough attention is paid to customer onboarding, users may **sign up without fully understanding the product's value,** leading to lower activation and retention later on.

However, this isn't just a conversation about conversion rates. It's also about customer quality. Identity verification (IDV) ensures that your signups are genuine users, which often correlates with higher customer lifetime value (CLTV). Without proper checks, you may attract high volumes of users, but many could be low-value or even harmful—like fraudsters exploiting your product. So it's a balance between quantity and quality that every business must calibrate for its specific context.

A good onboarding rate for **B2B** free trial or freemium products is between **40–60%.** A good onboarding rate for **B2C** products is between **30–50%** (Source: InnerTrends).

Among SaaS companies, the **average activation rate** – the percentage of new users who reach the activation milestone with their product journey – is **37,5%** (Source: Userpilot).

A good onboarding rate for **B2B** free trial or freemium products

40-60%

A good onboarding rate for **B2C** products

30-50%

Average activation rate among Saas companies

37.5%

Collaboration between compliance officers, product managers, and user experience (UX) designers is key here, so that **KYC requirements are built into the UX by design** rather than ‘slapped on’ as a legal formality.

When done right, an onboarding flow can both **satisfy regulators and delight users.**

Simplifying and clarifying the steps:

One of the golden rules of onboarding is to keep it **as simple as possible.** Each additional form field or document request is a potential drop-off point. In fact, if you notice an above-average drop-off during sign-up, it likely means you’re asking for too much information too soon.

Audit your verification steps and remove any that aren’t absolutely necessary for **initial onboarding.**

01

For required steps, make them **clear and concise: explain to users what you need and why.**

Across financial services, an estimated **63% of potential new customers never finish signing up.**

Lack of understanding is a major cause of abandonment – many consumers don't grasp why a service needs so much personal data just to open an account.

To address this, provide brief explanations or tooltips (e.g. "We ask for ID to comply with anti-fraud laws and to keep your account secure").

02

Also, **consider breaking the process into logical stages** rather than one long form. Studies have found that **splitting sign-up** across multiple pages can **increase completion rates**, because it feels less overwhelming (Source: HelpScout)

03

Use a **progress indicator** to show users where they are in the process, but ensure it moves at an encouraging pace – research shows people are **twice as likely to abandon a form** if the progress bar starts off moving slowly, whereas a quickly advancing progress bar motivates completion (source: Sardine.ai)

04

Each step should be straightforward: use plain language (avoiding jargon), and if possible, pre-fill or automate data entry.

For example, if you can scan an ID document to capture

info, don't make the user type it all in. Pre-filling fields using data the user already provided (or using APIs to pull data) can save end-users from repetitive typing and speed up onboarding

The overall goal is to **minimize friction.** Every minute saved and every confusion eliminated directly boosts the chances a user finishes verification.

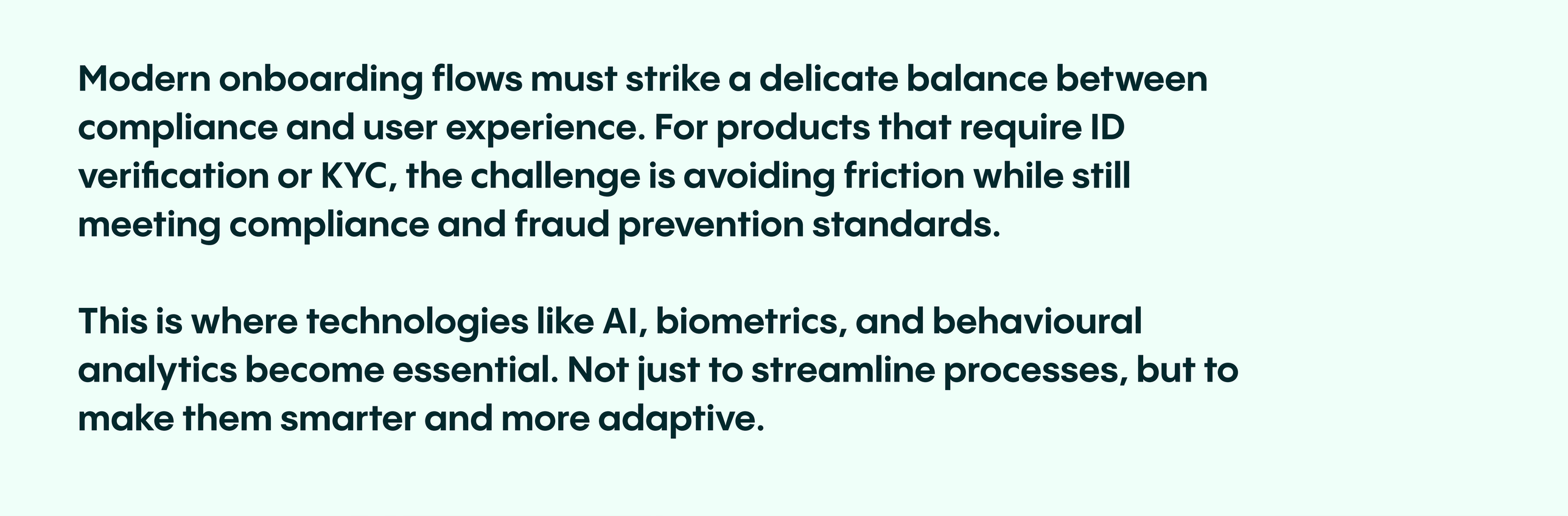
A guiding question: **Do we absolutely need this field or step?** If yes, implement that improvement.

2/

Make customer onboarding your competitive advantage by leveraging AI, automation and biometrics

Modern onboarding flows must strike a delicate balance between compliance and user experience. For products that require ID verification or KYC, the challenge is avoiding friction while still meeting compliance and fraud prevention standards.

This is where technologies like AI, biometrics, and behavioural analytics become essential. Not just to streamline processes, but to make them smarter and more adaptive.



01 – Automated ID verification:

Use AI-powered document verification services like Veriff to check IDs quickly and accurately. Veriff can validate an ID's authenticity in seconds by analyzing security features, and perform facial matching to ensure the person is the ID owner.

By automating what was once a manual review, you both speed up the process and reduce human error. And this could represent a huge factor in optimizing your process and reducing costs. In fact according to our KYC guide data:

→ Banks typically employ **10 % of the workforce** in financial-crime-related activities.

→ Average periodic reviews for low-risk customers can **take 100 minutes to complete.**

→ **Over half of the costs associated with KYC are people-related costs.**

→ Research shows that customers drop off when onboarding takes more than 19 minutes, and so today's financial services must aim for excellent KYC quality within that precious time frame.

And this is true also for non-financial services related businesses.
For instance, Stake, the biggest online cryptocurrency casino, had a slow verification process. The cumbersome onboarding process could take weeks when it was not automated, causing a substantial drop-off in customer engagement and revenue.
“Veriff is so much faster than our manual in-house solution. It would be embarrassing to share how much faster it is!” says Dan Richardson, Chief Product Officer, Easy.go

Another example is Gana777, a global gambling operator with a mixture of digital sites and land-based casinos in sites across Europe, Africa and the Americas.
“Our fraud rates have decreased and our conversion times have come down considerably - where before we would say to a customer that we would get back to them in 24-48 hours to validate their account, we can now do it in less than a minute,” says Erick Sapién, Country Manager, Gana777

Aim for an ID verification step that takes only a couple of minutes (depending on the complexity and risk related to the industry). For example **an ID check with Veriff takes around 6 seconds**, a benchmark to strive for. If you find your process is taking, say, 30 minutes or requires 1 or 2 day of waiting for approval, **that’s a big red flag**: you likely need to automate more.

02 – Biometrics and liveness:

Leveraging device cameras for biometric checks can add security without adding extra steps for the user. A quick selfie or short video can be used to verify liveness (ensuring the person is real and present) and even match their face to the ID.
Modern liveness detection can happen in less than a second – for example, by having the user smile or blink for the camera – and can thwart fraudsters using stolen IDs.

This is far less effort for the user than, say, having a video call with an agent for verification (which some banks used to require), having to recall personal information to answer security questions, or remembering a password. It also creates a sense of modern, high-tech security. Always inform the user this is to protect their identity – framing it positively can improve their willingness to comply.

03 – Behavioral analytics and AI risk scoring:

Advanced behavioral biometrics can run in the background during onboarding to flag suspicious activity **without changing the user flow.**

For example, software can look at how the user fills the form – monitoring typing speed, mouse movements, device and location consistency – to predict if it's likely a genuine user or a bot/fraudster.

If something looks very anomalous (e.g. an impossibly fast typing speed or an unusual IP geolocation), the system could trigger additional verification steps or a manual review for that case, while genuine users sail through. This adaptive approach ensures **legitimate customers face minimal friction**, while potential bad actors get challenged early on.

For example, this might mean 95% of users see a simple 2-step verification, whereas a risky 5% might be asked to provide an extra document or go through a secondary check. AI-driven risk models thus help maintain security without making the standard path onerous for everyone.

Source: Veriff

04 – Seamless integration & customer support

Ensure your technology integrates well and works across devices. A frictionless verification not only improves conversion but can even be a selling point (“Sign up securely in minutes!”).

As one customer onboarding best-practice says: “Automate what you can” to create **a streamlined, frictionless experience** for your customers.

→ **Mobile optimization** is critical – many users will complete IDV on their phone even if they start on desktop (for instance, scanning an ID is easier with a phone camera).

→ Design a **handoff mechanism** (QR code or secure link) so a user can switch to mobile to complete verification and then back to desktop, or vice versa.

→ Also, choose **IDV tools that integrate with your app or web seamlessly** (through SDKs or APIs) to avoid redirecting users to external sites unnecessarily. A **cohesive, in-app experience feels more trustworthy and keeps users focused.**

By harnessing these technologies, you can make **verification fast and user-friendly.** The ideal outcome is that users barely perceive the "security checks" as a hassle – instead, it feels like a natural part of onboarding.

A frictionless verification not only improves conversion but can even be a selling point ("Sign up securely in minutes!").

Last but not least, try to have a fast and reliable customer support process for all of the users that are going through onboarding.

42% of customers will return to a service after a good experience, and a whopping 90% will return and recommend it after a great support experience.

When you're guiding users through something as sensitive as ID verification, providing excellent support (clear instructions, help on standby, quick issue resolution) can turn a wary first-timer into a long-term advocate.

On the other hand, **+50% of consumers** will switch to a competitor after **only one bad experience** (Source: Zendesk).

42%

of customers will return to a service after a good experience

90%

of customers will return and recommend it after a great support experience

+50%

of consumers will switch to a competitor after only 1 bad experience.

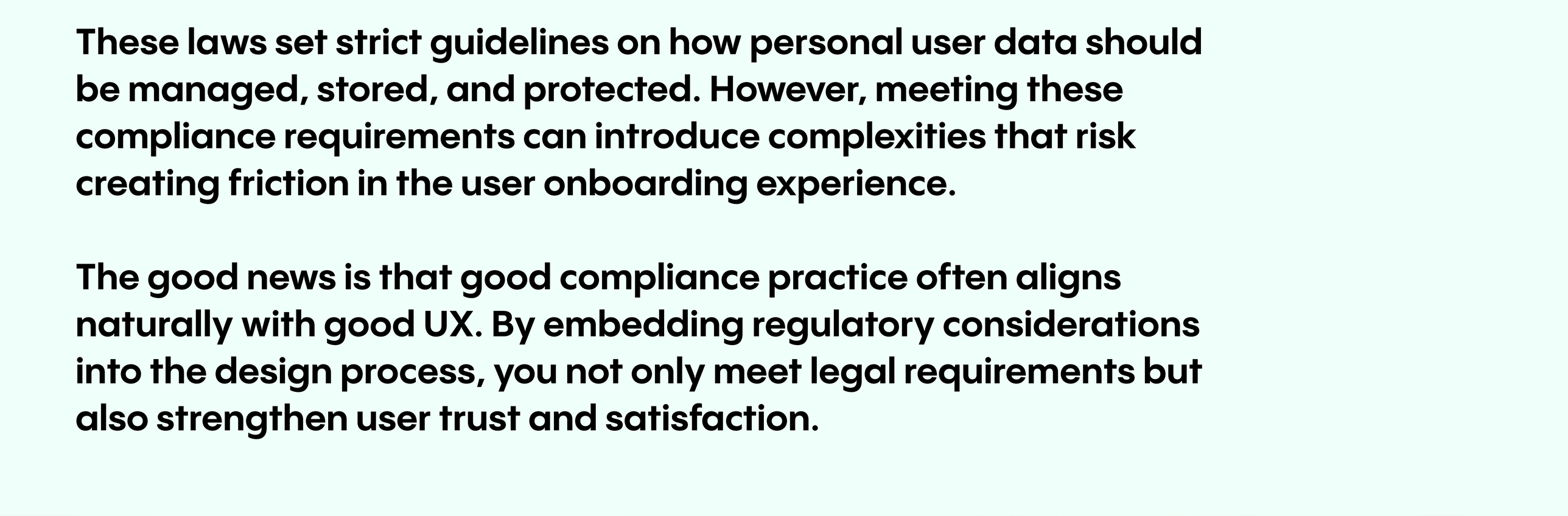
3/

Best practices for regulatory compliance and data protection without sacrificing UX

When developing digital products requiring identity verification (IDV) and know your customer (KYC) processes, regulatory compliance—such as data protection and anti-money laundering (AML) laws—is mandatory, not optional.

These laws set strict guidelines on how personal user data should be managed, stored, and protected. However, meeting these compliance requirements can introduce complexities that risk creating friction in the user onboarding experience.

The good news is that good compliance practice often aligns naturally with good UX. By embedding regulatory considerations into the design process, you not only meet legal requirements but also strengthen user trust and satisfaction.



01 – Privacy by design and data minimization

"Privacy by Design" means proactively integrating privacy considerations from the outset rather than addressing them as afterthoughts.

"Data Minimization" complements this by ensuring you collect only the essential information required to complete identity verification and remain compliant.

Implementation suggestions:

→ Carefully **evaluate every data field requested during the onboarding process**, asking if it is genuinely required for verification purposes. For instance, while social media profiles or secondary phone numbers might have marketing value, they are typically unnecessary for compliance (while also increasing onboarding friction) and can thus be omitted or deferred .

→ **Clearly communicate** the necessity of sensitive data like Social Security Numbers (SSN) or passport details, explaining their legal relevance to compliance obligations. **Transparency helps users understand that such requests aren't intrusive but mandatory.**

→ **Automatically delete or anonymize user data** after a reasonable timeframe, aligning with privacy principles of data minimization and storage limitation. Informing users about this practice can also gently encourage them to finalize their onboarding.

Benefits:

Adopting data minimization results in shorter, less intimidating onboarding forms, creating a simpler and more positive user experience. Users also appreciate visible respect for their privacy, which significantly reduces hesitation or abandonment during onboarding.

02 – Secure data handling

Regulatory compliance mandates not only specify what data can be collected but also strictly dictate how securely it must be stored, transmitted, and processed.

Implementation details:

→ **Always encrypt sensitive data** in transit (using secure protocols like HTTPS) and at rest within databases.

→ Access to sensitive personal data should be strictly limited to only **those personnel who require it to perform their job functions**, complemented by **comprehensive audit logs for accountability.**

→ When partnering with **external ID verification providers, verify their security standards** through certifications such as ISO 27001, GDPR compliance. Check out the Veriff Trust Center.

→ Clearly communicate your rigorous data security standards to users in **straightforward, trust-building language**. For example, mentioning "secure encryption" during the onboarding process can reassure users, making them more comfortable uploading sensitive documents.

Benefits:

Communicating robust data handling practices builds trust with users, reassuring them that their sensitive data is secure, ultimately increasing their willingness to complete onboarding. Compliance with data security regulations also reduces the risk of fines and legal liabilities.

03 – Clear communication about data use

Transparency about data usage is crucial for regulatory compliance (especially GDPR and other privacy laws) and directly impacts user trust and onboarding success.

Implementation details:

- During onboarding, **clearly articulate why each piece of requested data is needed**, how it will be used, who will access it, and how it is securely stored. Simple statements like "Your information is required for identity verification in compliance with AML laws and will not be shared or sold" can significantly ease user concerns. Always make sure that such statements reflect your actual data processing practices.

- Be upfront about **checks against AML sanctions lists or politically exposed persons (PEP) lists,** presenting them as standard regulatory procedures to normalize the experience for users.

- If user data is shared with **third-party verification vendors or credit bureaus, you should explicitly disclose this** and assure users of the compliance standards upheld by these partners.

- Provide **easily accessible privacy notices and consent requests**. Users appreciate straightforward, jargon-free explanations about their data handling, the lawful basis for data processing, and the possibility of exercising their rights, such as requesting data deletion.

Benefits:

Transparent communication reduces user uncertainty and fear about data misuse, resulting in higher onboarding completion rates. Regulatory compliance is also supported by documented evidence that users have been appropriately informed.

04 – Minimizing required information (tiered KYC approach)

Concept:

Collecting the minimal required information upfront, with additional data gathered later as needed, enhances compliance and UX simultaneously.

Implementation details:

→ Adopt a tiered or risk-based approach to compliance, asking for basic ID verification for initial user onboarding or low-risk scenarios. Then you can start asking for **more information** and/or **collecting additional documents** (such as proof of income or address) only **when users reach higher thresholds or pose higher compliance risks.**

→ Clearly define and **regularly review the minimal compliance requirements** to avoid unnecessarily extensive data collection.

→ Create a **structured checklist** with your compliance team to challenge every **data field requested during onboarding**, aiming to remove anything not necessary for your activities. Consider also strictly, what is explicitly required by law.

Example

A currency exchange app might initially require only basic ID for transactions under a specific threshold (e.g., $300). Higher verification steps become necessary only when users want to exceed standard transaction limits.

Benefits:

Using a tiered approach simplifies onboarding, particularly for casual users, significantly reducing abandonment rates. Regulatory authorities also favor risk-based approaches that limit unnecessary data collection.

4/
Case studies

To wrap up, let’s look at some real-world examples and data points that highlight the impact of optimizing onboarding (especially with IDV/KYC) on user conversion and business success. These cases demonstrate how the best practices discussed above translate into measurable outcomes.

01 – Fintech and financial services

Juancho Te Presta

Full case study ↗

Juancho TE PRESTA

CHALLENGE

Juancho Te Presta, one of Latin America's fastest growing fintech platforms, was experiencing a high rate of customers getting stuck or abandoning the identity verification process. Nearly 29% of approved daily users could not complete verification due to friction and unclear next steps.

SOLUTION & IMPLEMENTATION

They integrated Veriff's identity verification tools, including video recording features to add transparency and reduce potential fraud. This real-time insight allowed them to pinpoint where customers were struggling and streamline the verification flow.

IMPACT

By smoothing out the identity check, Juancho Te Presta reduced friction for legitimate customers, resulting in higher completion rates and near-elimination of fraud. The combination of automated checks plus video analysis created a more secure yet user-friendly onboarding journey.

KEY RESULTS

→ **Drop in 'non completed' verifications**. Reduced from 29% to 18%—nearly a 50% improvement in a single week.

→ **Exceptional Fraud prevention.** Total fraud dropped to below 1%, enabled by clearer user verification and deeper insight through video captures.

01 – Fintech and financial services

Crown Agents Bank

Full case study ↗

Crown Agents Bank

CHALLENGE

Crown Agents Bank operates utilizes biometrics and identity verification in its pension payment service, which deals with an elderly demographic, where identity verification can be challenging. Previously, high abandonment rates and repeated attempts were causing poor user experiences, and their call centers were overwhelmed by support inquiries.

SOLUTION & IMPLEMENTATION

After A/B testing two providers, Crown Agents Bank selected Veriff. The trial proved Veriff's superiority in both ease of onboarding and fraud detection. With Veriff's KYC solution, Crown Agents Bank migrated away from manual, error-prone processes to a streamlined, digital-first workflow.

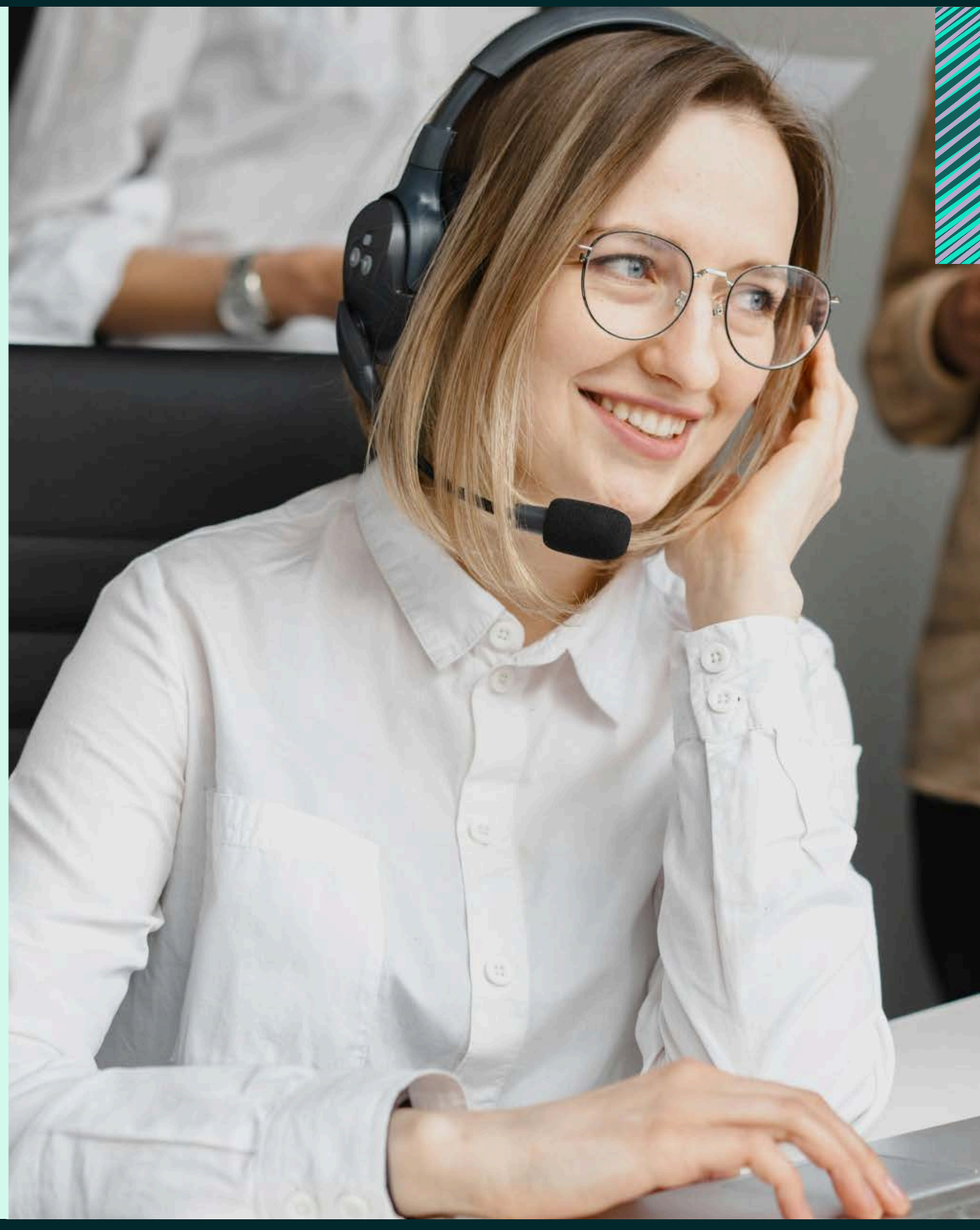
IMPACT

By partnering with Veriff, Crown Agents Bank strengthened compliance with global regulations, cut user onboarding times, and improved cross-border transaction security. Fewer calls to customer support, faster onboarding time and nearly zero-abandonment clearly show how a robust, digital-first KYC flow can foster both regulatory compliance and positive user experiences.

KEY RESULTS

→ **90% Online KYC completion rate.** Exceeded the initial 20% goal, reaching an 80–90%"digital uptake, described internally as "phenomenal" by the company.

→ **Near-100% onboarding success.** Abandonment in the verification process dropped to near-zero, drastically reducing friction for end users.



02 – Digital marketplaces

EMD

EMD MUSIC

Full case study ↗

CHALLENGE

EMD, a digital music distributor, was facing a growing fraud issue. Bots and fake identities were being used to claim royalties, creating compliance concerns and damaging trust with artists and platforms. Their manual identity verification process was slow and ineffective—taking days to resolve cases and failing to prevent abuse.

SOLUTION & IMPLEMENTATION

EMD integrated Veriff's identity verification (IDV) solution to automate the client onboarding process and detect fraud early. Veriff's biometric verification and global document coverage allowed EMD to instantly verify artists' identities and identify duplicate or suspicious accounts at the very first step.

IMPACT

Veriff's solution drastically reduced friction for legitimate users, enabling a seamless and trusted onboarding experience for artists worldwide. The move also strengthened EMD's credibility with streaming platforms by taking clear action against fraud and ensuring regulatory alignment in multiple jurisdictions.

KEY RESULTS

→ **Issue resolution rate.** Veriff helped eliminate 90% of onboarding issues instantly.

→ **Reduced Time-to-verify.** Reduced identity verification time from 2–3 days to under one minute.

→ **Real time Fraud prevention.** EMD now detects and prevents fraudulent duplicate accounts in real-time.

02 – Digital marketplaces

Legitify

Legitify®

Full case study ↗

CHALLENGE

Notarization is traditionally a manual, face-to-face process. For businesses conducting cross-border transactions, this created a major bottleneck. Legitify needed a way to offer remote, compliant identity verification across jurisdictions without slowing down user workflows.

SOLUTION & IMPLEMENTATION

Legitify partnered with Veriff to embed biometric ID verification directly into their platform while still in beta. Veriff's global reach, regulatory expertise, and EU-compliant biometric verification aligned perfectly with Legitify's target market in legal and financial services.

IMPACT

Veriff's trusted infrastructure allowed Legitify to grow quickly, build trust, offering users a smooth verification process while maintaining strict legal compliance. The partnership reassured customers that digital notarizations were both secure and trustworthy, key for high-stakes legal and financial workflows.

KEY RESULTS

→ **Enhanced scalability.** Enabled rapid expansion into new markets from day one with a single provider.

→ **Global compliance coverage.** Supported secure transactions across hundreds of countries without needing multiple vendors.

→ **Seamless UX.** Delivered a frictionless identity verification experience critical to Legitify's value proposition.