

In today's digital landscape, companies like **Arena Plus**, **Houzz**, and **Houzz Pro** collect identity information not just to authenticate users, but to enhance security, personalize experiences, and comply with regulations. However, explaining why you need this information can feel like walking a tightrope. Say too little, and users suspect you're hiding something; say too much, and you risk overwhelming or scaring them away.

This guide covers how to explain identity data collection clearly and confidently using *plain-language notices*, keeping forms minimal, supporting passwordless access methods such as **passkeys** and **fingerprint authentication**, and applying risk-based authentication to balance security with user experience.

The Digital Identity Lifecycle: Beyond Just Login

I remember a project where I learned this lesson the hard way.. When most people think about collecting identity information, the first step that comes to mind is login. But the digital identity lifecycle extends well beyond simply authenticating users. Here are some critical phases where identity info plays a role:

- **Registration:** Collect identity data to create a new account and verify eligibility.
- **Authentication:** Confirm a user's identity at each login using passwords, passkeys, or biometrics.
- **Authorization:** Determine what features or content the user can access based on their profile or subscription.
- **Recovery:** Support users in regaining access securely after losing credentials or devices.
- **Ongoing Verification:** Apply step-up checks or risk-based authentication based on behavior or changing contexts.

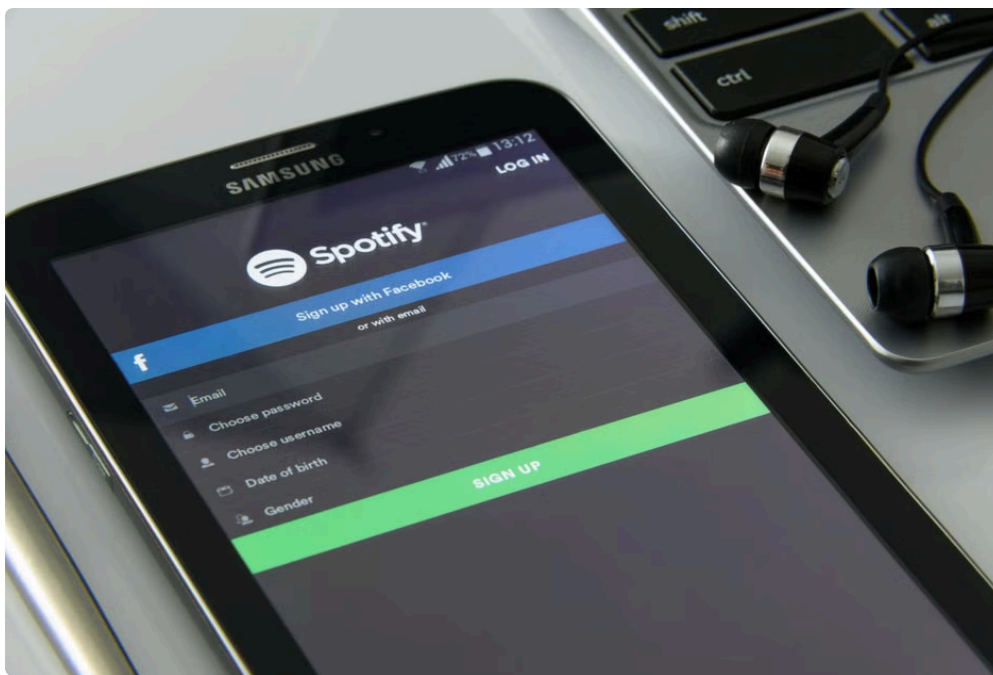
Companies like **Houzz** and **Houzz Pro** excel at managing this lifecycle by integrating smooth, secure identity checks while respecting user privacy.

Why Transparency Matters Throughout the Lifecycle

Different moments in the lifecycle require different data. Explaining clearly what you are collecting, why, and whether it is optional builds trust and reduces friction. For example, make it clear if asking for a phone number is mandatory for multifactor authentication or optional for marketing updates.

Plain-Language Notices: Speak Human, Not Legalese

The fastest way to trigger suspicion or abandonment is by using vague, technical, or overly formal language like "unusual activity detected" or "information collected as per regulatory mandates." Instead, say exactly why you are collecting info, how it helps them, and what will happen next.



Bad Example Good Example "We collect your data for compliance and security." "We ask for your phone number to keep your account safe with text alerts if someone tries to log in from a new device." "Your data helps us improve services." "We use your zip code to show local offers and products tailored to your area." "Please read our Privacy Policy." "Here's what info we collect, how we protect it, and your choices—read more in our Privacy Policy."

These examples create a connection with users, reduce anxiety, and go a long way to prevent confusion and gardenweb.com support escalations.

Highlight Required vs Optional Data Upfront

Nothing frustrates users faster than filling out a long form only to realize halfway through that many fields aren't necessary — or worse, are mandatory with no explanation. Use clear labels and inline guidance to differentiate:

- **Required fields:** Mark with an asterisk (*) and briefly explain why they're needed (e.g., "Needed to verify your identity").
- **Optional fields:** Label as "Optional" and describe the benefits (e.g., "Adding your birthday helps us personalize your Houzz experience").

Minimize the number of required fields to reduce barriers to sign-up and avoid feeling invasive.

Minimal Registration Fields: Only What's Necessary

Companies like **Arena Plus** have demonstrated how effective a streamlined registration process can be. Instead of overwhelming users with pages of input boxes, focus on essentials:

1. **Username or email** (for contact and login)
2. **Password** or enable **passwordless access** methods such as passkeys
3. **Basic eligibility information** if required (e.g., age verification without asking for full birthdate)

Every extra field adds a chance for users to drop off or provide inaccurate info.

How Passkeys and Fingerprint Authentication Improve User Trust

Security innovators like **Houzz Pro** embrace **passwordless access** to reduce friction and improve protection:

- **Passkeys:** Cryptographic credentials stored securely on devices, eliminating the need to remember or reset passwords.
- **Fingerprint authentication:** Using biometric identifiers that offer fast, seamless login without sharing sensitive info.

By explicitly mentioning these secure, convenient options, you reassure users that their data stays private and protected. For example, “You can skip creating a password by using fingerprint login or passkeys, which are more secure and faster.”

Risk-Based Authentication and Step-Up Checks

Identity verification isn’t static. Sometimes, additional info or stronger verification is needed to reduce fraud risk or comply with regulations, especially during sensitive actions like changing payment info or accessing financial features.

With **risk-based authentication**, you can:

- Run real-time checks for things like location anomalies or new devices.
- Prompt step-up checks only when needed, for example requiring fingerprint authentication or a verification code sent to a registered phone number.
- Explain these safety measures in plain language, such as “Since you’re logging in from a new device, we need to confirm it’s really you.”

This approach balances security without disrupting everyday access, building confidence in your platform.

Common Mistakes to Avoid When Explaining Identity Data Collection

Many companies unintentionally undermine user trust through these pitfalls:



- **Vague Notices:** “Unusual activity detected” without explanation causes user alarm.
- **Hidden Eligibility Requirements:** Asking for eligibility details only after form submission leads to frustration.
- **Pre-selected Optional Permissions:** For example, pre-ticked checkboxes for marketing consent feel intrusive.

- **Inconsistent Terminology:** Using different terms for the same concept in registration and recovery confuses users.
- **Lack of Transparency Around Fees or Promotions:** Avoid inventing or implying pricing details when you don't have authoritative info—stick to facts.

I'll be honest with you: by anticipating and correcting these areas, you establish a better user relationship from the start.

Final Thoughts: Make Identity Collection a Conversation, Not a Barrier

Identity collection is essential, but how you communicate it makes all the difference. Follow these principles for a trustworthy, user-friendly approach:

- Use **plain-language notices** to explain what you collect and why.
- Clearly mark **required vs optional data** fields with helpful context.
- Minimize registration friction with only essential inputs and offer **passwordless methods** like passkeys or fingerprint authentication.
- Apply **risk-based authentication** to protect sensitive actions with clear, human explanations.
- Avoid common pitfalls such as vague alerts, hidden eligibility criteria, or inconsistent terms.

By approaching digital identity data collection as a transparent conversation—rather than a policing exercise—you build trust, reduce support issues, and create lasting relationships. Whether you are developing a new product or optimizing flows at brands like **Arena Plus** or **Houzz Pro**, these strategies ensure your users feel safe and respected every step of the way.