Change providers without losing control of your digital identity

Changing agencies involves more than the website's files. It raises a question of continuity: will the business be able to keep communicating, receive email and administer its accounts throughout the transition?

Published: 2 November 2026 · Updated: 2 November 2026

Could this happen to you?

Files are not enough. The website has been handed over, but the old agency still holds the accounts.

The website changes. What about email?. The redesigned site works. Incoming email has not been checked.

An old account remains active. The contract has ended. The former provider can still make changes.

WHAT YOU WILL BE ABLE TO CHECK

- Make an inventory of the services and the people responsible for them.
- Distinguish handing over materials, migrating services and closing old access.
- Check that the new arrangements work before completing the transition.

Contents

Start with the services, not the passwords 2

Separate the operations to understand their effects 3

Prepare a usable handover 4

Check the new arrangements before completing the transition 5

Sources and method 6

Your supporting document: a one-page memo, available with the guide online.

wize.lu/en/guides/change-providers-without-losing-control

STEP 1 OF 4

Start with the services, not the passwords

The aim: An overview of the services, accounts and people responsible.

Imagine a business changing agencies. It receives the website's files and thinks it has the essentials. Yet the domain, email and analytics management accounts may require separate access. This illustrative situation shows why a file delivery alone does not describe a handover.

Start by making an inventory: domain name, DNS management, hosting, website content, email, social media accounts and analytics tools. Add forms, sending services and subscriptions needed for the business to operate.

For each entry, record the account used, the person responsible, the billing arrangements and the person who can authorise a change. This overview helps identify dependencies before deciding what needs to move.

> **Definition**
>
> Here, handover capability means being able, in practice, to take back an activity that was delegated or entrust it to someone else. The arrangements need to be clarified with the provider.

> **KEEP IN MIND**
>
> **What to do now:** List the services to take over before asking for passwords.

STEP 2 OF 4

Separate the operations to understand their effects

The aim: A clear scope and timetable.

Changing who manages a domain, moving a website and changing email providers serve different purposes. These operations may be connected, but they should not be confused.

A domain name can direct users to several services. DNS Luxembourg explains the role of name servers in accessing connected services. Changes to their configuration therefore need to take account of every use of the domain, beyond the website alone. [1]

Operation	Question to resolve
Domain management	Who will be able to administer it and monitor renewal?
Website migration	Where will its content, data and functions be hosted?
Email migration	How will messages be retained and incoming and outgoing email maintained?

One provider may retain some services while the new provider takes over others. What matters is an explicit allocation, with a timetable and a contact for each operation.

KEEP IN MIND

What to do now: Separate the domain, website and email in the transition plan.

STEP 3 OF 4

Prepare a usable handover

The aim: Materials and permissions that can actually be used.

The following list is a preparation framework proposed by Wize. Adapt it to the tools actually used, your contracts and your business's responsibilities.

1. **Identify what needs to be handed over.** Files, exports, content, data, configurations and documentation: ask what will be delivered and in which format.
2. **Clarify usage rights.** Some themes, fonts, images or plugins may be subject to licences. Check which can continue to be used and which require a separate step.
3. **Prepare access for the incoming provider.** Prefer invitations or delegated access where available. Avoid sharing a password in a group conversation.
4. **Describe the handover.** Record the steps, the people who approve them and what to do if a check fails.
5. **Plan how earlier materials will be retained.** Define useful backups, who may access them and how long to retain them, according to your obligations and needs.

Keep a written record of what has been handed over and what remains to be done. A short list checked by both providers makes taking over easier than a set of files with no explanation.

KEEP IN MIND

What to do now: Specify the deliverables, authorisations and validation steps.

STEP 4 OF 4

Check the new arrangements before completing the transition

The aim: Continuity checked and access brought up to date.

Going live is a visible milestone, but incoming email, forms and administrative access also need to be checked. Plan appropriate tests: view essential pages, submit a test form, check it arrives and test incoming and outgoing email with the people involved.

Next, check that the business has the agreed permissions and that recovery contact details are up to date. ANSSI's guidance highlights the value of protecting access, including a second factor where possible. [2]

Once the new arrangements have been confirmed, remove permissions that are no longer needed according to the agreed timetable. If old access remains necessary during a follow-up period, specify its purpose and when it will be reviewed.

The record to keep

A closing record of the services taken over, checks completed, access still open and outstanding points. This document becomes the starting point for the next transition.

KEEP IN MIND

What to do now: Check the services, then record any access that remains open.

A controlled transition starts with an inventory, follows explicit responsibilities and ends with checks. The business retains a record of its digital arrangements, even when its partners change.

Sources and method

The sources support the passages that refer to them. Wize's practical lists and organisational guidance are presented as its own method. The opening situations are illustrative examples. Procedures should be confirmed with the providers involved. The reference source pages are in French. The French guide was updated on 2 November 2026.

1. DNS Luxembourg — FAQ, activation and name servers — The role of DNS servers and services connected to a domain.
https://dns.lu/fr/faq

2. ANSSI — Ten golden rules for digital security — Account protection and authentication.
https://cyber.gouv.fr/securisation/10-regles-or-securite-numerique/