JOINT POSITION PAPER · NOVEMBER 2026

Freedom of movement in digital Europe: opening the social internet up to competition

Joint position paper presented by startups and tech organizations building new, healthy social solutions.

This position paper was coordinated by the Modal Foundation



Introduction

If the EU wants people to be able to move freely from platforms like Instagram, TikTok and Facebook to European social media services, what stands in the way today? And what would consumers, builders, civil society and challenger services need from Brussels to make that a reality? This paper sets out to answer these questions in practical terms.

Builders across Europe are creating social apps without the dark patterns and unfair practices of the big platforms. People can already join them, but they cannot bring what makes a social network worth using: their identity, their content in a usable form, and the people they are connected to. The best a European user can get today is an incomplete zip file with some of their data, not including their social connections. What they can do with that data elsewhere is an open question.

This paper asks Brussels for one structural change. **Every platform should hold its users' data, connections and interactions in a personal data server built to one common standard**, so people can use whichever app they choose and keep their data and network. A working standard for this already exists and runs at scale. We ask the Commission to make it mandatory through the Digital Fairness Act, and to make the portability rules already in force work in the meantime.

IN BRIEF

- **A personal data server for every account**, under one enforced standard, with AT Protocol's PDS as the starting point. This is our core ask - it is the only system that puts users in control over their digital lives. Current solutions firmly favour platforms over users; we call on the Commission to change this once and for all. Vehicle: Digital Fairness Act, with the DMA able to set the standard for gatekeepers sooner.

Additionally, we ask the Commission to ensure the following:

- **Leaving must be no harder than joining.** Access criteria for the DMA's Article 6(9) portability tools set by the Commission rather than the gatekeeper, and a symmetry principle for every platform. Vehicles: DMA enforcement; Digital Fairness Act.
- **An end to practices that stop people finding each other elsewhere.** A ban on suppressing links and proofs to a person's accounts on other services and on restricting user-requested contact matching, and scrutiny of self-preferencing. Vehicles: Digital Fairness Act and the Unfair Commercial Practices Directive; DMA Article 6(5).

Why it’s needed

Europe has already solved this in other markets. When you change bank, your direct debits and standing orders move with you. When you change mobile provider, you keep your number, and the people who called you before can still reach you without knowing anything changed. This is true in technology as well: when you change ISPs you remain able to access the internet addresses and email services you used before. Moving between social apps should be just as seamless. Europeans have a right to take their data with them. That right should amount to freedom of movement between social networks: identity, connections, and content that travel intact.

The rules meant to provide that freedom fall short. The GDPR and the DMA require platforms to hand over a copy of people’s data, but in formats other services cannot easily use. The big platforms decide which challengers may use the transfer tools that do exist. And neither law requires platforms to hand over people’s connections and interactions in a form that works elsewhere. That leaves switching costs in place, so competition in social media stays closed and people have little real choice.

As builders of challenger apps, we encounter these problems over and over again. The current rules, as enforced, do not enable competition. We are part of a growing movement building social media where your identity, content and connections belong to you rather than to any one app. These apps, built on a common infrastructure of login identity, data servers and relays, allow people to seamlessly move between apps without losing anything.

The timing matters. The Commission’s April 2026 study on horizontal interoperability found it technically possible but declined to prioritise it, while the people building on open protocols have barely been part of that conversation. The Digital Fairness Act proposal is expected in Q4 2026. This paper is timed to reach policymakers while that proposal is being shaped, so that builders’ views help inform it.

Today: data you can download, a network you can’t take with you

The social graph, more than raw data portability, is the real blocker for people who want to move platforms. As builders, we see two major problems come up over and over again.

First, what’s technically offered under the GDPR and the DMA often doesn’t work in practice. Today, if you want to leave LinkedIn, Instagram, or Facebook, you can request your data under Article 20 of GDPR. What you get back is what one builder called “dead data”: lawful on paper, often incomplete, and useless for actually continuing your experience anywhere else. When we tested it, exporting from Instagram took sixteen steps, and on X,

your followers come out as a list of numbers (see Appendix: Leaving Platforms, Step by Step). On LinkedIn, requesting the quick profile download first blocks you from requesting the full archive for two hours, and the quick download looks complete but leaves out positions, skills and education. GDPR gives you the right to take your data with you, but says nothing about what that data has to look like or how fast it has to arrive, so platforms can comply on paper while the export remains practically unusable.

For the largest platforms, the Digital Markets Act already goes further. Article 6(9) requires designated gatekeepers, including Facebook, Instagram and LinkedIn, to provide effective, free, continuous and real-time portability. LinkedIn has built export tools in response, and Meta offers direct transfers to approved services. But these tools are only open to services the platform approves, and would-be competitors have to go through arbitrary administrative processes. The equivalent would be switching bank accounts before open banking reforms. Platforms that aren't designated as gatekeepers, like X, fall outside the DMA entirely.

Second, even when an export does work well, it still does not solve the social network problem. Leaving a platform means losing the network of people you have built up, and a data file, even if continuously updated, does not bring that network with you. Even the gatekeepers' tools leave out the people you're connected to. On all three platforms we tested, your content travels with you in some form, but your followers do not.

In social media and the social internet in general, your network is the one part of an account you cannot rebuild on your own. Connections, friends and followers should be able to travel with the user, with the consent of the people on the other side, and not stay locked in a platform. This is necessary for consumer choice, and a must if Brussels is serious about opening social media to competition.

What we want: a personal data server for every account

Every social media platform should hold users' data, connections and interactions in a manner compatible with a standard interface known technically as a "Personal Data Server" or "PDS". This system guarantees that data are at all times controlled by users. Data can be public or private, with access to it already authorised according to how they have already chosen to share it on social media. This personal data server must follow a common standard that ensures compatibility across applications on the social internet. The relationship between the user and a platform becomes as follows:

- For every user, the platform creates a universal digital identifier so that accounts can be identified outside of the platform.

- User-generated data include content (posts, articles, photos, videos, events), social connections (follows, friends), interactions (likes, reposts, remixes) and transactions (subscriptions, bookings).
- All these data are recorded on the user's personal data server.
- Other applications on the social internet can access that data when authorised by the user (consent-driven data access) and process them in ways that match the sharing choices the user has already made (public post, private account, limited to a group).

This is a fundamental shift from the current model, where user data are locked inside each platform, a model that by definition favours platforms over citizens and forecloses competition. Implemented, it would open up user choice and market competition in a way that is impossible today. It solves the network lock-in problem described above: identity, connections and content stay in a space the user controls instead of being exported as a copy, so moving between apps does not mean starting over.

In this system, nobody has to leave anything. Your existing Instagram account would be exposed through a Meta-hosted PDS, mapped in a way that respects your privacy settings. People on Flashes (a European Instagram alternative) could see your posts straight away, and you could find and follow Flashes users from inside Instagram. If you later preferred the feeds on Flashes, you could use that app instead, and nobody on Instagram would notice a difference when you post. If you stopped trusting Meta to host your data, you could move your account to another host, just as you keep your number when you change mobile provider. Nothing would change for the people you are connected to.

One standard, open to every protocol. We recommend that Brussels adopts the PDS used by the AT Protocol as the common standard (it is currently a draft standard within the IETF). It has already been proven at scale and is used across a large, diverse range of applications. Choosing it does not mean making a choice between protocols. A PDS that can hold ActivityPub accounts is already being explored and, similar to how Meta or Linkedin can implement the PDS standard, any other application can do the same.

Note: the AT Protocol PDS currently only supports public data in production; however private data is in testing as of publishing and expected to enter production in late 2026 or early 2027.

What the standard must guarantee. Good standards have been let down by bad implementation, often deliberately, before. GDPR privacy protection and data portability rules have been undermined by dark patterns used in consent cookies and data downloads. We must ensure this does not happen again. The PDS standard should be enforced in a way that ensures the following:

- **A legible data standard**, so that different apps and services can easily read and use the data a person has created on any platform.

- **Clear, user friendly designs**, so that users can easily use their PDS with any app implementing the standard.
- **Guaranteed PDS portability**, so that users can change PDS providers at any time with no penalty.

A test for the effectiveness of implementation of the standard is if it is as easy, or easier, for a user to use a new app with their data and connections as it is to sign up to an incumbent platform. We provide an illustrative example of what this might look like here.

For the avoidance of doubt and in anticipation of pushback from the market dominant platforms, we must emphasize that any issues with user consent can be easily solved with, e.g. a dual opt-in approach.

It already works

AT Protocol shows this approach works at scale. Bluesky, the largest app built on it, reports more than 45 million registered users, and says people use more than a thousand different apps built on the protocol every week, all drawing on the same accounts and data.

The dominant platforms already do a version of this for their own products. Threads content appears directly in the Instagram feed, and users move between the two without realising they are looking at a separate app. Meta now also offers a single account that works across its apps. If a platform can build that kind of integration for its own products, the capability to extend it to others already exists. What matters is the conditions.

It has also been done across companies before. Until 2015, Facebook let third-party apps access a user's friend list through its API, and a Facebook account could be used to sign into a wide range of other apps and services. It withdrew that access. The current gap isn't capability. Platforms have no incentive to open that door, and no law requires them to.

Platforms might argue that sharing data is safe inside one company but risky outside it. EU law has already dealt with that argument once: Article 7 of the DMA requires messaging gatekeepers to open up to rivals while preserving their level of security, including end-to-end encryption.

We must emphasise that it should be up to each user to control how their data, social graph and social media activity is used - it should not be subject to the approval of any one app or platform. Any system where the existing dominant platforms decide where a user can take their social identity is one that favours platforms.

Builders are ready to compete

Builders are already offering people something better. Flashes is a photo and video app on the AT Protocol, built and hosted in the EU. What you post there is visible in any AT Protocol app that chooses to display it. You pick your own feeds, and in most of them what you see comes overwhelmingly from the people you follow. On Instagram, by Meta's own reckoning, only 7% of time spent goes to what Meta calls "content from friends". Sifa, also on the AT Protocol, is a professional network where your career history lives in your own account. mu is an AT Protocol microblogging service hosted in Europe with a focus on high quality news. Sill gathers the most popular links shared by the people you follow on Bluesky and Mastodon, so you can keep up without scrolling the feeds themselves. Newsmast, on ActivityPub, brings curated communities and feeds together across the fediverse.

People clearly want better options. As research from the Future of Technology Institute (FOTI) documents, tools like One Sec, Opal, AppBlock, and the Brick device have been downloaded or bought millions of times, because people are willing to spend money, time, and effort to make their current platform less addictive.

Our asks

Our asks fall under two legal vehicles. The Digital Fairness Act is the structural track: a new law, expected as a proposal in Q4 2026, that can establish the right to take your network with you and set rules for every platform. Enforcement of the Digital Markets Act is the near-term track: the obligations already bind designated gatekeepers, and the Commission can act on them now without new legislation. Neither track depends on the other. The DMA work should start immediately; the DFA should carry the standard.

Digital Fairness Act

ASK 1

Establish the right to take your network with you. The DFA is the EU's consumer protection response to unfair digital practices, including dark patterns and services that are made hard to leave. Being unable to leave a social app without losing your network is a consumer harm of the same kind. The DFA should require social media platforms to hold users' data, connections and interactions in a personal data server that follows one common, enforced standard, with AT Protocol's PDS standard as the starting point and the guarantees set out above. For gatekeepers, the DMA could set the standard sooner.

ASK 2

Leaving a platform must be no harder than joining it. Dead data and obstructive export flows are an unfair practice, and they reach platforms the DMA does not cover, such as X. The DFA should set a simple symmetry principle for every platform, gatekeeper or not: leaving a platform or exporting your data must be no harder than joining it, and making it harder should count as an unfair practice.

ASK 3

Ban practices that stop people finding each other elsewhere. Even where tools to help people move exist, platforms work against them. A basic “find your friends elsewhere” feature, matching who you follow on one platform with who they are on another, would make moving far easier. But platforms like X explicitly prohibit this kind of account matching in their terms of service, and competitors avoid building it for fear of being sued. Platforms also suppress outbound links, which makes it harder for any tool, including ones that help people find each other on a new platform, to reach anyone. Some builders work around this without any platform cooperation: Sifa, for example, lets members verify their LinkedIn profile by posting a proof on it with a tool called Keytrace. The proof is then saved as a signed claim in their own AT Protocol account. That only works for as long as LinkedIn allows the proof and link to stay on the profile. A platform should not be able to use its control over a person’s existing network to stop that person finding the same people somewhere else. The DFA should:

- add the removal or suppression of profile links and proofs that point to a person’s accounts elsewhere to Annex I of the Unfair Commercial Practices Directive;
- bar restrictions on user-requested contact matching;
- apply both bans to the terms users agree to and the terms developers agree to.

Digital Markets Act enforcement

ASK 4

Make Article 6(9) portability work now. Builders who have tried to use the DMA's Article 6(9) tools have hit barriers set by the gatekeepers themselves. For example, to get access to LinkedIn's portability API, a developer needs a LinkedIn Company Page, business verification with a registered legal entity and business email, and LinkedIn's approval. The access is bundled, covering messages, contacts and invitations, so a service that only needs some of that data cannot ask for less. The obligation exists; what is missing is a specification of what compliance means. Using its power under Article 8 to specify the measures a gatekeeper must take, the Commission should:

- set proportionate access criteria for Article 6(9) tools itself, with input from an independent standards body, rather than leaving the gatekeeper to set them;
- require gatekeepers to offer granular scopes, so services request only the data their users need;
- define "effective, continuous and real-time" portability as real-time sync of content and connections, in a form other services can act on and with the user's permission.

ASK 5

Examine self-preferencing inside the network. The big platforms give their own products the visibility they deny to everyone else. Meta surfaces Threads content directly inside the Instagram feed, giving an unfair advantage over separate apps. Article 6(5) prohibits gatekeepers from ranking their own services more favourably than those of third parties. The Commission should examine whether surfacing Threads content inside the Instagram feed is compatible with that obligation.

What our asks would look like: Visual

Illustrative mockups of a personal data server in use. Platform names show where data would be hosted; interfaces are simplified and unbranded, and all figures are fictional.

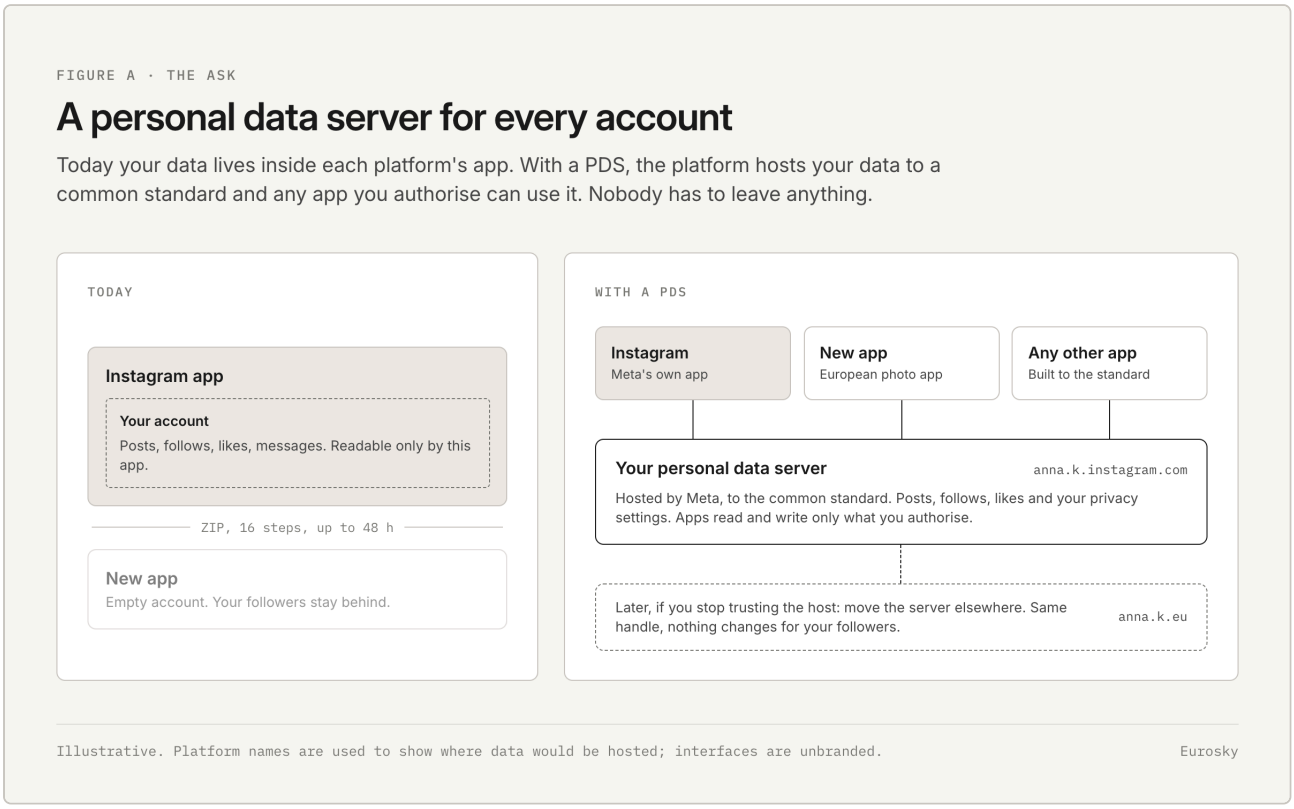
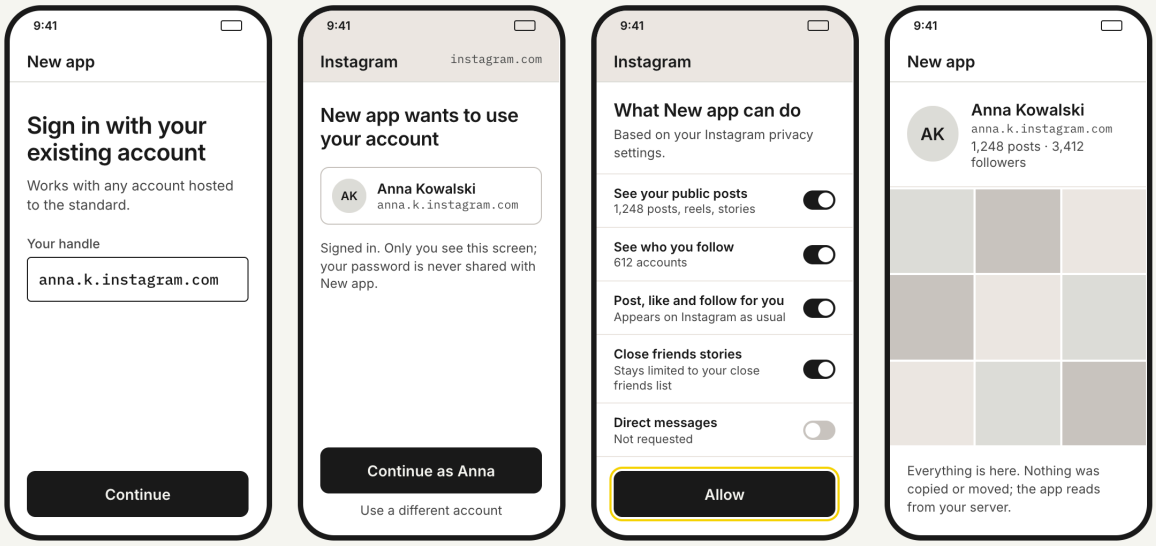


Figure A. The ask: a personal data server for every account. Today's silo compared with a platform-hosted PDS that any authorised app can use.

FIGURE B · USING A NEW APP

Signing in to a new app with your Instagram account

The authorisation flow that AT Protocol apps use today, with Meta as the host. Privacy settings you already chose on Instagram carry across; there is nothing new to consent to.



01 · NEW APP

Type your handle. The app finds your host from it.

02 · INSTAGRAM

You're sent to your host to confirm it's you.

03 · INSTAGRAM

Review what the app can do. Your existing privacy choices set the defaults. Allow.

04 · NEW APP

Your posts, followers and follows are already there.

4
steps, one Allow, about a minute

0
files downloaded, accounts moved or followers lost

1
account, usable in every app built to the standard

Illustrative mockup based on AT Protocol OAuth. Interfaces are simplified and unbranded.

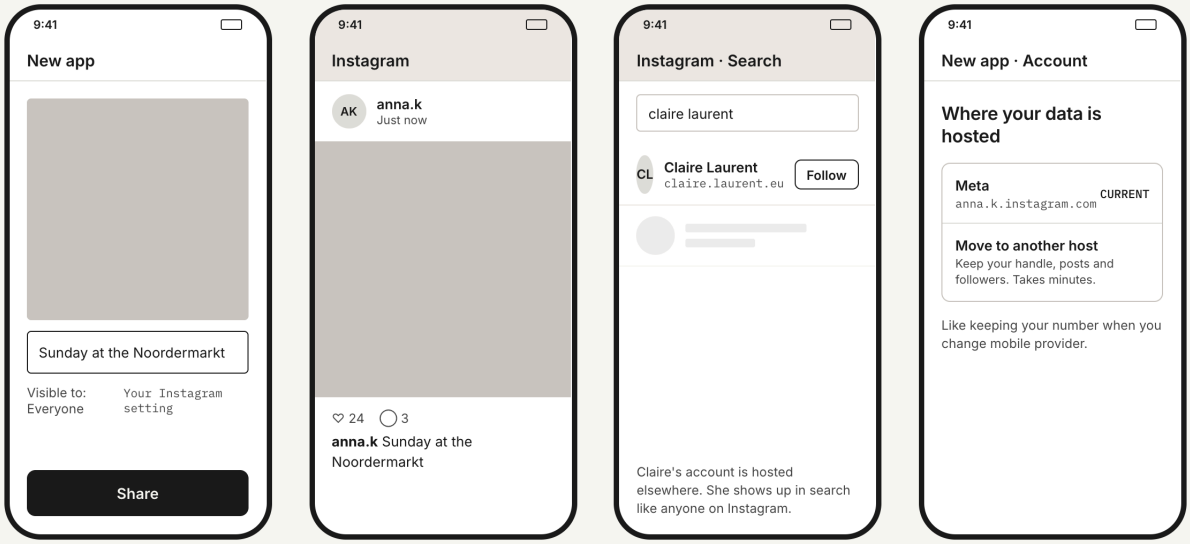
Eurosky

Figure B. Signing in to a new app with your Instagram account, using the authorisation flow AT Protocol apps use today. Existing privacy settings set the defaults.

FIGURE C · ONE NETWORK

Apps become interchangeable; the network stays the same

Anna uses the new app. Her friend Jonas stays on Instagram. Neither notices a difference.



01 · ANNA, NEW APP

Anna posts from the new app. It writes to her server.

02 · JONAS, INSTAGRAM

Jonas sees it in his Instagram feed, like any other post.

03 · JONAS, INSTAGRAM

Jonas finds and follows someone who only uses the new app.

04 · ANNA, NEW APP

If Anna stops trusting Meta, she can change host. Her network doesn't notice.

Illustrative mockup. Interfaces are simplified and unbranded.

Eurosky

Figure C. One network: a post from the new app appears on Instagram, an Instagram user follows someone on the new app, and the account can change host without the network noticing.

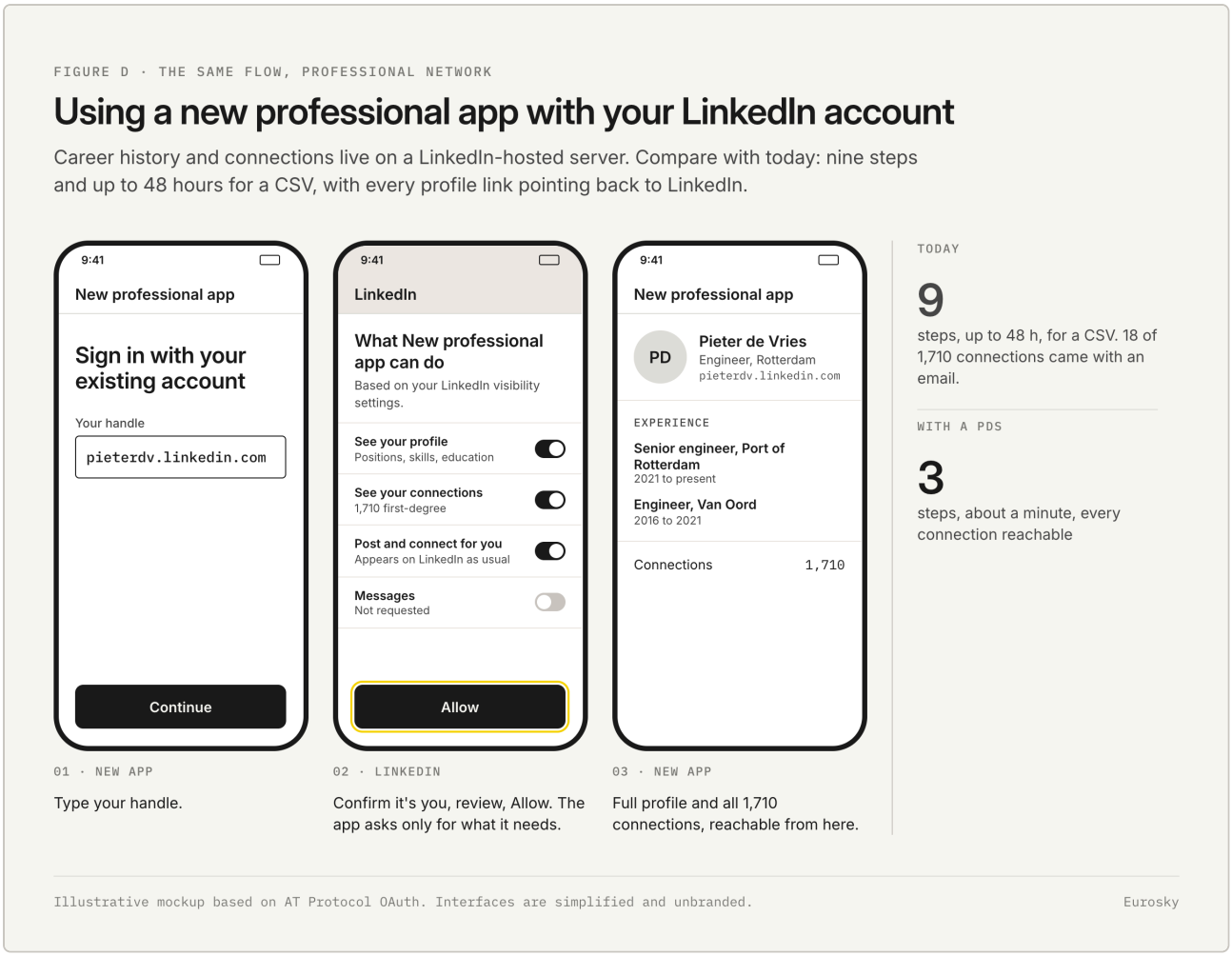


Figure D. The same flow for a professional network, with career history and connections on a LinkedIn-hosted PDS, compared with today's nine-step export.

Closing

Europe already guarantees people the right to switch banks or phone providers without starting over. Social media should be no different. A personal data server for every account would give people real freedom of movement on the social internet: the right to choose which apps they use, without losing their content or the people they are connected to. In the meantime, making the existing portability rules work and ending the terms that stop people finding each other elsewhere would start to open the market now.

European policymakers have a simple choice: give citizens real digital autonomy, or leave control with the platforms.

European builders can't compete with gatekeepers on the current rules. They need to be in the room as Brussels decides what comes next, rather than brought in after the decisions are made.

Appendix A: Leaving Platforms, Step by Step

Under GDPR Article 20, users have a right to data portability. For the largest platforms, Article 6(9) of the Digital Markets Act goes further: gatekeepers must provide continuous, real-time portability, including to third parties the user authorises. This is the route open to challenger services today: with a user's permission, they can ask a gatekeeper to send that user's data directly to them.

We tested what this means in practice on LinkedIn, Instagram and X in September 2026. The table below compares what each platform gives you when you leave: how long it takes, what comes with you, and what doesn't. On all three, your content travels with you in some form, but your followers do not.

	LinkedIn	Instagram	X
Steps to export	9	16	10
Time to receive data	Up to 48 hours in our test; link expires after 72 hours	Not published by Meta; within 24 hours in our test; ZIP download link expires after four days	Not published by X; about 24 hours in our test; download link expires after seven days
Your content	Profile, posts and messages, as CSV files	Posts, reels, stories and messages, with captions, media and timestamps	Posts, media, message text and likes; bookmarks excluded
Your followers and network	First-degree connections with name, profile URL, company and position; emails only where shared	Followers and following as usernames and account IDs, no contact details	Followers and following as numeric IDs with a profile link on X; no usernames
Direct transfer tool	API for approved third-party apps (EEA users only)	Transfers to Meta-approved destinations	None
DMA gatekeeper	Yes	Yes	No
Can your followers move with you?	No	No	No

LinkedIn

It takes nine steps to get a list of contacts you can only reach through LinkedIn. See the step by step process here.

After going through this process, the full archive took up to 48 hours to arrive, and the download link expired after 72 hours. The Connections.csv file lists each first-degree connection's name, profile URL, company, position and the date you connected, but not where they are based. Email addresses appear only for connections who have chosen to share theirs; in our test export, 18 of 1,710 connections came with one. Second- and third-degree connections aren't included at all. What you end up with is a list of who you know and where they work, but every profile link points back to LinkedIn, and there is no channel to your network on any other platform.

Instagram

Exporting your data from Instagram means sixteen steps across the app and Meta's Accounts Centre. See the step by step process here.

Meta doesn't publish how long an export takes. We sent ours to Google Drive through the "Export to external service" option, in HTML format. The first time we tried to open the finished export, Meta showed an error saying the page wasn't available; the next time it arrived within 24 hours. Had we downloaded it to our device instead, we would have had four days to download the ZIP before the link expired.

Posts, reels and stories come through with full captions, media and timestamps, and direct messages come through with full text. Followers and following lists are included, but only as usernames and account IDs with a connection date: no contact details, and no route from that list back to those people on any other platform. The archive includes likes and comments you gave on other people's content, but not the likes or comments your own posts received. What you authored travels with you; what connects you to other people, and how they responded to you, does not.

X (formerly Twitter)

Downloading your data from X takes ten steps, and your followers come out as numbers. See the step by step process here.

X doesn't publish how long an archive takes. Ours arrived in about 24 hours, but reported times range up to several weeks for accounts with a long history. The download link isn't in the email itself: X attaches the instructions as a PDF. You must download the archive while logged in to the same account on the same device or browser, and the link expires after seven days.

Your posts come through with timestamps and full-resolution media, along with direct message text (missing where the other person deleted their side) and your likes. Bookmarks are left out entirely, so anything you saved rather than posted doesn't come out at all. Most importantly, the follower and following lists record people by numeric user ID, with a link to

their profile on X, but no usernames or names. The only way to find out who someone is means clicking through to X one account at a time, or using third-party tools to look them up in bulk. By contrast, the archive does list the advertisers who have targeted you, by username. X is not designated as a gatekeeper under the DMA, so it has no obligation to offer anything better.

What direct transfer tools add

LinkedIn, Facebook and Instagram are designated as gatekeeper services under the DMA, and both companies offer routes that go beyond the download archive. X has not been designated, so it has no equivalent obligation. For X users, the archive above is all there is.

LinkedIn offers a Member Data Portability API, which it says it provides in response to the DMA. With a member's consent, an approved third-party app can pull a snapshot of that member's LinkedIn data, including posts, articles, connections and the people they follow. It can also pull a running log of new activity, such as posts, comments and reactions, starting from the moment of consent. The log only goes back 28 days, so an app has to keep checking to stay current. Only members in the European Economic Area can consent. To get access, a developer needs a LinkedIn Company Page, business verification and LinkedIn's approval.

Meta's tool, Export Your Information, works the other way round. It pushes data to destinations Meta has approved, through the "Export to external service" option in Instagram's export settings. Photos, videos and posts from Facebook, Instagram and Threads can be transferred directly, and on a recurring schedule. To become a destination, a service must be vetted through the Data Transfer Initiative's Trust Registry, hold a verified Meta business account, integrate with the open-source Data Transfer Project, and pass Meta's own review and testing.

For content, this is progress. Meta in particular has built most of what click-to-switch would need for posts and media. Both tools share the same limits, though. The platform decides which services can connect. And neither moves a network in any usable form. LinkedIn's API returns your connections' names, jobs and employers, but no way to reach them outside LinkedIn. Meta's followers and following lists travel only inside the general file archive, as the same list of usernames an ordinary user downloads. Neither offers any way for the people you are connected to choose to follow you somewhere new.