dacros

A FREE DACROS CARD

Moving to EU-hosted services

The readiness checklist

What to have ready before you move email, files, calendars and accounts from a US-based provider to one based and hosting in Europe. Most of a move is preparation, and the order matters: work down the card and tick each line.

EDITION
Edition 1 · November 2026

FOR
Businesses moving email, files and accounts from a US-based provider to a European one

ONLINE
dacros.com/resources/eu-hosted-services-readiness-checklist

Before you choose

- [ ] **Run the data location check first,** so you know what you are moving, and why: dacros.com/resources/data-location-check
- [ ] **Read each candidate's own pages** for the company's country, where it stores data, and its data processing agreement. The UK has adequacy regulations for every EEA country, and for Switzerland [1].
- [ ] **Check the contract.** A processor's work for you must be governed by a contract, and at the end of the service it must delete or return your data, at your choice [2].
- [ ] **Check the import and the export:** what the new service can import (mail, calendars, contacts, files) and in which formats, and what the old one exports, and until when after you cancel.

The inventory

- [ ] Every mailbox, shared mailbox, alias and group address, and who uses each one.
- [ ] Every shared drive and folder, its owner, and who it is shared with, people outside the business included.
- [ ] Calendars, including shared ones and any for rooms or equipment.
- [ ] Every service people sign in to with the old account, using a "sign in with" button. Those logins stop working when the account goes.
- [ ] Devices and apps set up with the old account: phones, laptops, and the scanner or any app that sends email.

DNS and email records

- [ ] **Who controls the domain's DNS,** and that you can log in to it.
- [ ] **A copy of every current record:** MX, SPF, DKIM, DMARC and any verification records. A screenshot or an export will do.
- [ ] **The new provider's records,** ready to enter: MX, SPF and DKIM, and a DMARC policy [3].
- [ ] A day or more before the switch, lower the time to live (TTL) on the records you will change, so the change takes effect sooner.

Mailboxes and files

- [ ] Export each mailbox and keep the export until the checks after the move have passed.
- [ ] Copy files with their folders, and list the sharing you will need to set again: sharing does not travel with a copy.
- [ ] Decide what stays behind. An old archive may be better kept as an export than moved.

Sign-in and two-step login

- [ ] An account for each person, protected from the first sign-in by a passkey or by a strong password with two-step verification [4].
- [ ] At least two administrators, with recovery details that do not lead back to the old account.
- [ ] The password manager updated, and the old entries marked for removal.

Staff

- [ ] Tell everyone the date, what changes for them, and what to do first on the morning after.
- [ ] Give each person a short sheet: how to sign in, set up two-step login and add the account to their phone.
- [ ] Warn them about messages asking them to “confirm” or “re-verify” their account around the move.

The cut-over, and the checks afterwards

- [ ] Choose a quiet time, and stop changes on the old service.
- [ ] Change the MX records, then the rest. Make a final copy of anything that arrived during the switch.
- [ ] **Check:** mail in and out, from inside and outside the business and from a phone; calendars and contacts; shared files open for the right people; the scanner and any app that sends email.
- [ ] **Check the domain** with the NCSC’s email security check, which tests whether it is set up to the standards in the NCSC’s email guidance [3, 5].
- [ ] Keep the old service until every check has passed and a full export is stored safely. Then close it, and ask for the deletion your contract provides for [2].

Sources

[1] ICO, Is the restricted transfer covered by adequacy regulations?, checked 10 November 2026 · ico.org.uk

[2] UK GDPR, Article 28, Processor, paragraphs 3 and 3(g), checked 10 November 2026 · legislation.gov.uk/eur/2016/679/article/28

[3] NCSC, Email security and anti-spoofing, checked 10 November 2026 · ncsc.gov.uk/collection/email-security-and-anti-spoofing

[4] NCSC, Small organisations guide to cyber security: secure your important online accounts, published 9 April 2026, checked 10 November 2026 · ncsc.gov.uk

[5] NCSC, Email security check, checked 10 November 2026 · emailsecuritycheck.service.ncsc.gov.uk