EUROPEAN DATA PROTECTION SUPERVISOR

AUDIT REPORT ON THE EUROPEAN COMMISSION'S EU LOGIN MOBILE APPLICATION

EDPS case number 2019-0467

Brussels, 03 November 2025

Executive summary

Introduction

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of the Regulation (EU) 2018/1725[1] (the "Regulation") responsible for:

- monitoring and ensuring the application of the provisions of the Regulation and any other EU act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by an EU institution or body; and
- advising EU institutions and bodies and data subjects on all matters concerning the processing of personal data.

To these ends, the EDPS fulfils the duties provided for in Article 57 and exercises the powers granted in Article 58 of the Regulation. Among his powers to investigate, the EDPS can carry out investigations in the form of data protection audits. The power to audit is one of the tools established to monitor and ensure compliance with the Regulation.

Scope of the Audit

The remote mobile app audit concerns the privacy and data protection compliance of mobile applications for which EU institutions, bodies, offices and agencies (EUIs) act as controller or joint controller. It is the follow-up to the EDPS' 'Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions' (*the mobile apps guidelines*).

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

This thematic targeted audit assesses the alignment of mobile apps of the EUIs with the Regulation and Directive 2002/58/EC (*the ePrivacy Directive*). For the practical implementation, the EDPS' recommendations made in the mobile apps guidelines provided a standard.

Considering factors such as app audience (public or non-public mobile app), use case (diverse processing operations), user base (popular apps for larger impact), and controller resources (spearhead the efforts towards better app privacy with larger controllers), the EDPS selected four mobile apps to audit. The processing of personal data and privacy of users using EU Login mobile app is the specific scope of the present report.

This audit gathered evidence directly from the EUI controllers during a kick-off meeting as well as from technical tests on the concerned mobile apps. These tests were carried out in the EDPS lab and consisted in a static analysis of the mobile app's source code as well as performing a dynamic analysis to observe data in transit and data at rest. At the same time, the audit team downloaded manually the relevant policy documents and created clean versions that only contain the text for later review.

The comments and feedback received from the EUIs are included in the audit report and were taken into consideration where relevant.

The EU Login mobile app is a component of EU Login authentication services, previously known as the European Commission Authentication Service (ECAS). EU Login is used for accessing various European Commission services and other IT systems that require secure authentication.

For services demanding two-factor authentication, users can leverage the EU Login mobile app, developed by the Directorate-General for Informatics of the European Commission, and available for download on app stores.

After downloading the app on their mobile device, users need to initialise it by linking it to their EU Login account. The app offers multiple authentication methods: PIN code verification if user's device has access to internet connectivity, QR code verification if offline, and the 'On Mobile' method if accessing a service on the same mobile device that has the EU Login app installed.

Key findings of the audit

This report summarises the findings identified for the EU Login mobile app during the audit:

- *Lawfulness of processing* (Article 5 of the Regulation): The processing of personal data in the context of the EU Login mobile app is meant to provide secure access to EU online services and is thus based on Article 5(1)(a) of the Regulation. The EDPS has found that the storage of and the gaining access to information in EU Login users' mobile devices is limited to what is strictly necessary to ensure the provision of the service. It thus falls under an exemption of Article 5(3) of the ePrivacy Directive, in line with Article 37 of the Regulation.
- *Information to data subjects* (Article 15 of the Regulation): The Privacy Statement applicable to the processing entailed by the use of the EU Login mobile app provided data subjects with

partially unclear or incomplete information, in particular as far as the distinction between the general service of EU Login and the mobile app is concerned.

- *Record of processing activities* (Article 31(1) of the Regulation): Most of the required information was included by the European Commission in the record of processing activities. However, some elements should be reviewed, and where necessary complemented - such as the (categories of) personal data specifically processed by the mobile app and the role of third parties in the processing.
- *Governance and role allocation* (Article 29(3) of the Regulation): None of the documentation provided by the European Commission qualifies Google LLC, the provider of the Firebase Cloud Messaging push notifications service used for the EU Login mobile app, with respect to its data protection role in the context of the processing resulting from the use of the EU Login mobile app.

Recommendations and follow-up to the audit

The EDPS has thus issued a series of recommendations, which must be implemented by the European Commission within the timeline indicated in the audit report in order to ensure compliance with the Regulation.

The recommendations concern the documentation of the lawfulness of the processing of self-registered users' personal data, compliance with the principle of transparency and the controller's obligation to provide in-formation to data subjects, as well as with the controller's obligation to maintain a record of pro-cessing activities in the context of the processing of personal data of users of the EU Login mobile app. In addition, other recommendations address the allocation of data protection roles to the stakeholders involved in the processing of personal data resulting from the use of the EU Login mobile app.