

APPENDIX 1**RECORD OF PROCESSING ACTIVITIES (USER DATA– EU REGION)****1. Data controller:**

1. Facebook Ireland Limited

2. Data controller's DPO:

1. [REDACTED]@fb.com

3. Purpose of the processing:

We use the information we have (subject to choices users make) as described in the Data Policy (<https://www.facebook.com/policy.php>) to provide and support the Facebook Products and related services described in the Facebook Terms and Instagram Terms, including to:

1. provide, personalise and improve our Products.
2. provide measurement, analytics, and other business services.
3. promote safety, integrity and security.
4. communicate with users.
5. research and innovate for social good.

4. Categories of data subjects to which the personal data relate:

Individuals who visit, access, use or otherwise interact with products and services of Facebook (including for the avoidance of doubt, Facebook and Instagram).

5. Categories of personal data:

The personal data transferred is the personal data generated, shared and uploaded by or about individuals who visit, access, use or otherwise interact with the products and services of Facebook (including Facebook and Instagram). This includes:

1. information related to the things users do and the information users provide when using the services (such as profile information, posted photos and videos, shared location information, communications between users, and related information about use of the products and services);
2. information related to the data subjects that other users of the products and services provide (such as a user's imported contacts or photos);
3. information related to users' networks and connections (such as a user's connections to groups, pages, and other users);
4. information related to payments (such as information related to purchases or financial transactions);
5. information about devices (such as information from or about the computers, phones or other devices where users install software provided by, or that access products and services of, Facebook);
6. information from websites and apps that use products and services of Facebook (such as information about visits to third-party websites or apps that use a "like" or "comment" button or other service integrations); and
7. information from third-party partners (such as information related to jointly offered services or use of third party services); and information from affiliates of Facebook

and companies in the Facebook family of companies.

Such data may include:

8. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation; and
9. genetic data and biometric data (as those terms are defined in the GDPR) for the purpose of uniquely identifying a natural person.

6. Categories of data subjects to which the personal data relate:

Individuals who visit, access, use or otherwise interact with products and services of Facebook (including for the avoidance of doubt, Facebook and Instagram).

7. Categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations:

Sharing of user data is in accordance with the Data Policy. Data may be shared with the following recipients in accordance with the Data Policy, depending on the nature of the information – see Data Policy for details(<https://www.facebook.com/policy.php>).

1. Audience chosen by users.
2. Public audience.
3. Content others share or re-share about users.
4. New owner.

Sharing with Third-Party Partners

5. Partners who use our analytics services.
6. Advertisers.
7. Measurement partners.
8. Vendors and service providers.
9. Researchers and academics.
10. Law enforcement or legal requests.
11. Facebook Companies

8. Transfers of personal data to a third country or an international organisation:

All categories of data mentioned above may, potentially, be transferred to a third country, depending on the nature of the data and the use of the Product.

9. Where possible, the envisaged time limits for erasure of the different categories of personal data:

We store data until it is no longer necessary to provide our services and Facebook Products, or until an account is deleted - whichever comes first.

10. Where possible, a general description of the technical and organisational security measures referred to in Article 32(1):

The following information provides an overview of the security measures designed and implemented by Facebook to protect its systems, including the physical, technical, and administrative controls

that govern access and use of Facebook's systems.

Technical and Organisational Measures:

Physical security

Measures include the following actions to prevent unauthorised access to equipment processing or using data:

1. physical access to Facebook facilities is monitored by guard staff 24x7;
2. all individuals must identify themselves to security personnel in order to be admitted to the Facebook premises (or certain areas thereof). This requires a Facebook-issued photo badge with an electronic access code;
3. there are documented processes in place for the issuance of Facebook badges; the possession as well as the return of such badges is tracked and verified;
4. visitor logs are kept, and visitors receive temporary badges and must be accompanied by a Facebook employee to be admitted to areas beyond the Facebook premises' reception;
5. only authorised Facebook employees, vendors, and contractors that work in the Facebook premises are issued access badges for these installations; and
6. standard security measures observed, which are typical on Facebook premises, are composed of known technologies and follow generally recognised best practices for the industry, including electronic access systems with card readers, alarm systems, interior and exterior cameras as well as extensive security personnel.

Logical access and security

Strict policies are in place to address and limit access to production systems. For certain data access tools, tool owners authorise the nature and extent of access privileges prior to granting access. The procedures for requesting and generating certificates to access data for development and production are documented.

We also take the following actions to prevent the unauthorised use of data-processing equipment:

7. a formal protocol to grant or deny access to Facebook resources. Various access restrictions help to make access secure and limited;
8. one-time personnel identification, strong passwords and periodic reviews of access lists are in place to ensure that personnel accounts are put to their intended uses;
9. authorised access to internal support tools is controlled by means of a permissions service developed and distributed by Facebook;
10. the certificates grant personnel access based on role and is password protected in a restricted system. For certain restricted systems, dual-factor authentication is required;
11. unique personnel IDs are used to authenticate to systems;
12. passwords are configured to enforce password length and complexity; and
13. login history and failures are tracked.

Additionally, Facebook takes the following actions to ensure that the parties authorised to use a data processing system only have access to the data for which they have been specifically cleared, and that stored data or data being processed cannot be read, copied, changed or removed:

14. authorisation for Facebook services is enforced at all times and at all levels of a given system, with access rights being granted or processed on the basis of the personnel member's job responsibilities / need-to-know, which is provided via workflow tools;
15. access to production systems is restricted to trained and specifically authorised personnel members. Such access is revoked in the event of an individual's

- dismissal or termination of employment;
- 16. security audits, to ensure vendors follow Facebook security guidelines and sets application and personnel security as key vendor contractual obligations; and
- 17. use of a centralised logging system. Access to the logging system is restricted to authorised personnel and the logs are protected from modification and deletion from non-admin personnel.

Technical security

We use a range of technical security measures to protect its systems:

- 18. servers and network traffic are monitored by both industry-standard and proprietary tools to detect and respond to any potential security breaches; and
- 19. monitoring servers using best-in-class instrumentation tools that log changes to the servers and detect signs of a potential compromise; and
- 20. using a combination of industry-standard sandboxing technologies and a sophisticated Network Intrusion Detection system to monitor network activity for signs of malicious activity. In addition, a team of security experts continually studies real-world attacks and develops threat intelligence about the attackers' tools and techniques so that security systems accurately detect indications of potential compromise.
- 21. TLS encryption is part of the standard security architecture at Facebook. Core transport services require encryption, such as SSH or HTTPS, to exchange information;
- 22. encryption technology is used to provide security for online user authentication and administrator sessions;
- 23. remote data access to production equipment requires a link to the company's Intranet, which is subject to a dual authentication mechanism;
- 24. a VPN connection is necessary for personnel to access certain internal resources remotely
- 25. changes to the infrastructure and back-end environment, including changes to security tools,
- 26. follow the Facebook coding and release process;
- 27. all committed code changes are reviewed by an individual that is different than the developer and are tested prior to commit to production
- 28. Facebook uses a firewall configuration policy, which defines acceptable services that may be used in Facebook's environment. Only required ports and services are open. Changes to the firewall configuration are subject to review by the network and security personnel.

Organisational security and training

In addition, the Facebook provides employees and contractors with education and training on specific technical and organisational security measures:

- 29. Facebook employees are required to complete computer-based training on data protection and privacy and security that includes privacy and security by design, vendor security audits, privacy, laws and regulations, corporate policies and key privacy principles, and security awareness best practices.
- 30. All newly hired employees and contractors are required to complete training in privacy, security, ethics, and confidentiality.
- 31. Facebook's security team conducts company-wide security awareness activities to reinforce information security practices and policies.