Local laws and practices affecting compliance with the Clauses

Clause 13

Clause 12

Clause 7

Clause 4

Clause 2

Controller to Controller

Standard Contractual Clauses

The data importer will transfer Personal Information or Personal Data to provide, secure and monitor the Services in accordance with the Controller-Controller Data Agreement. Personal Information or personal data including information relating to individuals provided to the data importer via the Services by (or at the direction of) the data exporter or at the direction of the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

The Parties agree that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with his/her substantive and procedural rights to seek remedies in accordance with the data protection laws and regulations of the country of origin of the personal data and the General Data Protection Regulation (the "GDPR") provided such remedies are not rendered ineffective by any measures adopted by the data subject.

Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party incurs as a result of the breach of these Clauses.

The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting data subject.

Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs for responding to the request or decline to respond.

The data importer agrees to make information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

The data importer agrees to review his/her own systems and processes with a view to ensuring that the personal data transferred and any onward transfers are in compliance with the Clauses and with the relevant laws and regulations of the country of destination; such notification shall include all information available to the importer.

In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a specific context, in particular when it is based on a legitimate interest relating to freedom of expression and other public interests of the importer.

Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) to the extent that the importer is a processor acting on behalf of the exporter, to the extent the importer is bound by the same obligations as the exporter under these Clauses;

(ii) where requests from a data subject are excessive, in particular because of their repetitive character;

(iii) to the extent that the importer is a processor acting on behalf of the exporter, to the extent the importer is bound by the same obligations as the exporter under these Clauses;

(iv) where requests from a data subject are excessive, in particular because of their repetitive character;

(v) if the importer is bound by a public authority's legitimate interest, which was not overriding in nature in relation to the data subject's interests and fundamental rights and interests; and

(vi) where the importer is bound by a public authority's legitimate interest, which was not overriding in nature in relation to the data subject's interests and fundamental rights and interests.

Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with the data protection laws and regulations of the country of origin of the personal data and the General Data Protection Regulation (the "GDPR") provided such remedies are not rendered ineffective by any measures adopted by the data subject.

Onward transfers of personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer, by completing the Appendix and signing Annex I.A.

The data exporter agrees to submit itself to the jurisdiction of the supervisory authority of the country of origin of the personal data and the competent supervisory authority of the country of export of the personal data. The Parties agree that this shall be the country of the entity designated in Annex I.A.

The Parties agree to be bound by the terms of the Appendix, which shall be annexed to these Clauses. The Parties further agree to provide the data exporter with the relevant contact person's name, position and contact details in Annex I.A.

The Parties agree to comply with the requirements set out in Article 28 of the GDPR in respect of the role (controller/processor) of each Party and the transfer of the personal data from the territory of the country of origin to the territory of the country of export.

The Parties agree to implement the necessary technical and organisational measures to safeguard the personal data transferred and to ensure that they are processed in accordance with the Clauses and with the relevant laws and regulations of the country of destination.

The Parties agree to implement appropriate technical and organisational measures to ensure the processing of the personal data and the exercise of the data subject's rights under these Clauses without undue delay and at the latest within one month of the receipt of the request.

The Parties agree to inform the data subject of any decision not to agree to the onward transfer of personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer, by completing the Appendix and signing Annex I.A.

The Parties agree to inform the data subject of the existence of a particular mechanism for resolving disputes arising from these Clauses, in particular the dispute resolution mechanism referred to in Articles 79 and 82 of the GDPR.
The transfer is made:

- to facilitate the provision of the relevant Services as described in the Agreement by Google and/or the use of the Controller Services by Data Importer and/or in the case of Google, for the purposes described in Google's applicable Privacy Policy.

The period for which the personal data will be retained, or if that is not possible, the criteria used to determine that period

- for transfers to subprocessors of Google, also specify subject matter, nature and duration of the processing

Not applicable.

C. Competent Supervisory Authority

- identify the competent supervisory authority(ies) in accordance with Clause 13
- To the extent the data exporter is in Ireland, or is located outside the EEA, the Irish Data Protection Commission. Where the data exporter is located in a member state other than Ireland, the supervisory authority of the member state in which the data exporter is located shall be the competent supervisory authority.

Annex II

Technical and organisational measures including technical and organisational measures to ensure the security of the data

Explanatory Notes:
The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/series of transfers.

The description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The data importer has implemented measures at least equivalent to the technical and organisational measures described below, in addition to any other measures specified in or supplied to Google in connection with the Agreement.

1. Information Security Policy

- importer has a documented information security policy which its personnel are aware of and comply with.

2. Organization of Information Security

- data importer has organised its operations in such a manner that it is clear as to which individual(s) in the data importer's organisation have responsibility for information security. Data importer identifies and documents all security processes to include, but not be limited to: information risk assessment; incident response; patch management; vulnerability monitoring; security awareness education and training for its personnel (as appropriate to its operations).

- data importer has controls to reduce the risk associated with outsourcing services, including but not limited to: specifying security and confidentiality requirements; restricting subcontractor access to only those areas of the system(s) that are necessary to perform the outsourced service(s); generating event logs on systems and networks that have been accessed; and analysing the event logs.

3. Physical and Environmental Security

- data importer executes measures necessary to limit the risk of operational disturbance, theft, natural disasters and unauthorised access to data.

- data importer ensures that only authorised users have physical access to the network, critical systems and applications, server rooms, communication rooms and work environments. Data importer provides secure protection for its physical facilities (e.g., through card readers, key cards or a limited reception area).

4. Communications and Operations Management

- to ensure the confidentiality, integrity and availability of data, data importer applies proper security controls.

4.1 data importer has controls in place to detect and prevent malicious code from being executed on any system. These controls are regularly updated, and the most recent versions of antivirus signatures are distributed as soon as reasonably practicable to ensure detection and prevention of malicious attacks.

4.2 data importer ensures that there are reasonable controls in place when backing up data, such as event logs and reviews of those; the backup media is encrypted, where possible, using strong encryption; backup restoration testing is performed regularly; and procedures are in place to ensure backup media will operate in the event of an emergency.

4.3 data importer ensures that all external entry points to network segments containing data have access controls in place.

4.4 data importer ensures that the databases and repositories containing data are protected from unauthorised access by using appropriate authorisation controls. The database and connections to the databases are encrypted.

4.5 data importer ensures that controls for the operating system and applications are in place to prevent unauthorised access to system documentation.

4.6 data importer has a secure electronic messaging system to prevent unauthorised access. All incoming and outgoing emails are scanned.

4.7 data importer has controls to prevent unauthorised access to external or internet exposed applications and the information in those applications.

5. Access Control

- data importer has in place formal processes and procedures to support the secure creation, amendment and deletion of user accounts.

5.1 access is only granted to individuals needing access in order to perform a certain role, function or responsibility.

5.2 data importer ensures that access control mechanisms based on passwords are enforced by automated means.

5.3 data importer has controls in place that enable review of user access rights with particular focus on 'privileged users' (e.g. sys administrator).

5.4 data importer ensures that remote access to systems and applications containing data are governed by appropriate authorisation (e.g., two-factor authorisation), and that such access is encrypted (e.g., VPN).

5.5 data importer ensures that only authorised users can connect to wired or wireless network segments, if such segments exist.

5.6 data importer applies a level of security for its own wireless network that is equivalent to the level of protection achieved using/VPN. Traffic supports strong encryption and strong authentication.

5.7 data importer ensures that access to operating system used to store or process data use secure logon mechanisms.

5.8 data importer has a policy in place to prevent the spread of information from mobile computing such as portable computers and smartphones.

6. External Operating of Applications and Maintenance of Applications and Services

6.1 data importer has security controls of software, services and systems that process or make data accessible.

6.2 data importer has processes and systems for patch management (where appropriate).

6.3 data importer ensures that web-based products are reasonably protected against attack.

7. Information Security Incident Management

- in order to maintain business operations data importer has a formalised security incident handling process in place.

8. Business Continuity Management

- data importer ensures that Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) are documented and tested on a regular basis in order to ensure operational continuity (to the extent necessary for its operations).

- for transfers to subprocessors, data importer describes the specific technical and organisational measures to be taken by the subprocessor to be able to provide assistance to the controller and, for transfers from a processor to a subprocessor, to the data exporter.

Not applicable.

Last modified: 27 September 2021