Last updated August 2022

Policy for Data Transfers Outside the European Economic Area

OVERVIEW

This Policy for Data Transfers Outside the European Economic Area (this "**Policy**") sets forth the privacy principles that Datarails follows with respect to transfers of personal information received from European, Israeli or UK individuals and clients (each a "**Regulated Market**" and a "**Regulated Transfer**", respectively) within the scope defined herein.

The European Union Regulation (EU) 2016/679 of the European Council (the "**GDPR**") applies to all Member States of the EU. Special precautions need to be taken when personal data is transferred to countries outside of the European Economic Area ("EEA"), i.e., in case of transfers to countries such as the United States, which do not provide EU-standard data protection.

Similarly, Datarails is involved with cross-border data transfers pursuant to the UK General Data Protection Regulation, tailored by the Data Protection Act 2018 and the Israeli Privacy Protection Law, 5741-1981 and the guidelines, directives and regulations promulgated thereunder.

ABOUT THE SCC

The EU Commission has published standard contractual clauses for data transfers (the "**SCC**")[1] and determined that organizations which use the SCC offer sufficient safeguards for cross-border data transfer as required by the GDPR. Accordingly, Datarails shall enter into a set of SCC with each Datarails sub-processor located in a non-adequate,[2] non-EEA jurisdiction, receiving Personal Data from the EU or the UK.

SCOPE

This Policy governs Personal Data received in a Regulated Transfer about individuals processed within certain information uploaded by company client to our systems, for the jurisdictions specified above.

Currently, this policy applies to ensure protection of Personal information that is transferred from a Regulated Market to non-EEA (or non-adequate) jurisdictions.

Notwithstanding the generality of the foregoing, this Policy hereby incorporates by reference the SCC, which are deemed to be amended to the extent necessary, so they operate:

a. For transfers made by a Data Exporter to a Data Importer, to the extent that Israeli Privacy Law applies to such transfers and require additional contractual clauses to enable such transfer to certain jurisdictions, specifically according to Data Transfer Regulations; or

b. To provide adequate safeguards for the transfers in accordance with Israeli Privacy Law.

[1] For the updated form of standard contractual clauses as approved by the EDPB please see here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

[2] A list of adequate, non-EEA countries is available on the European Commission website: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Last updated August 2022

DEFINITIONS

"**Datarails**" means Datarails Ltd. and Datarails Inc.

"**Controller**" means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or European Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or European Community law.

"**Data Exporter**" means a Controller that transfers Personal Data or enables the transfer of Personal Data from a Regulated Market (including a database in Israel) to a Data Importer outside of the Regulated Market;

"**Data Importer**" means an entity outside of a Regulated Market, acting either as a Controller or Processor, that receives Personal Data from a Data Exporter;

"**Personal Information**" or "**Personal Data**" means any information that identifies or could be used to identify an individual. Personal Information does not include information that is anonymized so as not to permit identification of the relevant individual. Notwithstanding the above, to the extent such information is deemed personal information or personal data in an EU member state or the UK, Datarails will treat such information as Personal Information under this Policy.

"**Processing**" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processor**" means the natural or legal person, public authority, agency or other body which processes personal data only on behalf of the Controller and as instructed by the Controller.

"**Sensitive Personal Information**" means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, physical or mental health condition, and data relating to offenses, and/or criminal convictions.

PRIVACY PRINCIPLES

SCC' Principles: Datarails will comply with the principles set out in the applicable set of SCC (Controller to Controller, or Controller to Processor clauses).

DATA INTEGRITY: Datarails seeks to ensure that any Personal Information held about individuals is accurate, complete, up to date and otherwise reliable in relation to the purposes for which the information was obtained. Datarails seeks to collect Personal Information that is adequate, relevant and not excessive for the purposes for which it is to be processed. Datarails employees and sub-processors have a responsibility to assist Datarails in maintaining accurate, complete and current Personal Information.

TRANSFERS TO THIRD PARTIES: Datarails will only transfer Personal Information about individuals to a third party who has entered into SCC with Datarails or otherwise complies with the SCC's onward transfer principles.

In the event that Datarails transfers Personal Information to third parties for their independent purposes, it will do so only in compliance with the onward transfer principles set out in the respective set of the SCC.

ACCESS AND CORRECTION: Upon request, and as required by law, Datarails will provide individuals with access to Personal Information about them, subject to permitted exemptions. Datarails will also take reasonable steps to allow individuals to review Personal Information about them for the purposes of correcting such information.

SECURITY: Datarails will take adequate precautions to protect Personal Information in its possession from loss, misuse, unauthorized access, disclosure, alteration and destruction.

ENFORCEMENT: Datarails has established internal mechanisms to verify ongoing adherence to this Policy, Datarails commits to resolve complaints about a person's privacy and/or collection or use of personal information. European Union citizens with inquiries or complaints regarding this policy should first contact Datarails at compliance@datarails.com.

CHANGES TO THIS POLICY: This Policy may be amended from time to time, in accordance with the requirements of European data protection laws.