FUJITSU Europe
DATA PROTECTION POSITION PAPER

Introduction

As a multinational company and a responsible business, Fujitsu in Europe and its affiliated companies collect, process, share and store Personal Data obtained from individuals, employees, customers, and other 3rd parties.

This document should be read in conjunction with the on-line Fujitsu Privacy Policy as can be found on Fujitsu.

For the purposes of this document, "**GDPR (General Data Protection Regulation)**"" refers to Regulation (EU) 2016/679 of the European Parliament and of the Council and "**UK GDPR**" has the meaning given to it in section 3(10) of the UK Data Protection Act 2018.

Objectives and Scope

This position paper has been prepared to demonstrate Fujitsu's commitment to protecting and respecting privacy.

Fujitsu will comply with all relevant local and international data protection legislation.

This position paper sets out Fujitsu's approach to "**Processing**" "**Personal Data**". These terms are defined as follows:

> **Processing** means activities including collecting, storing, adapting, analyzing, using, transferring, disclosing, archiving, deleting Personal Data in the broadest sense and as defined in appropriate local or regional regulations (and **Process, Processes, Processed** and **Processable** should be read accordingly).
>
> **Personal Data** means information that:
>
> - relates to an identified or identifiable living individual ("data subject"); and
> - is held either (i) on a computer or in other electronic or automatically Processable form; or (ii) in a paper filing system arranged to be accessible according to specified criteria.

Fujitsu Processes Personal Data regarding its employees and individual contract workers, customers and other third parties like partners and suppliers and other individuals in its business.

Compliance with data protection policies

All persons who Process Personal Data for or on behalf of Fujitsu and its customers, including contract workers as well as employees, are expected to comply with Fujitsu data protection policies. Failure to comply with these policies is a serious matter which may give rise to disciplinary sanctions, up to and including dismissal.

If any person believes that Fujitsu may not have complied with Fujitsu data protection policies or any applicable data privacy law like GDPR, such person should inform Fujitsu as soon as practicable by email.

Processing of Personal Data

Fujitsu is committed to protecting and respecting the privacy of data subjects when processing their Personal Data. Personal Data may only be Processed in compliance with Fujitsu's policies and (as applicable in the context of its role as either data processor or data controller) in particular:

- where Processing is based on an appropriate contract or other legal act that is binding on the processor and the controller;
- ensuring that, in accordance with the contract between Fujitsu and a data controller, Fujitsu assists the data controller in ensuring compliance with its legal and regulatory obligations, including auditing, responding to Subject Access Requests, and conducting Data Protection Impact Assessments, taking into account the nature of Processing and the information available to Fujitsu;
- only processes personal data on documented instructions from the data controller, including regarding transfers of personal data to a third country or an international organization;
- where relevant, Fujitsu will not engage another data processor without prior consent of any data controller and without putting in place the same data protection obligations as set out in Fujitsu's contract with the data controller;
- where appropriate technical and organizational measures are in place to ensure that Processing will meet contractual, legal, and regulatory requirements;
- where relevant, international transfers must be carried out lawfully (an explanation of Fujitsu's approach to international transfers is set out in the International Data Transfer Annex below);
- in a way which is fair, legitimate, and proportionate and there is a lawful ground for Processing;
- where applicable, only if consent is properly obtained and ensuring that Fujitsu has an appropriate record of the consent having been given;
- Personal Data must be retained in accordance with its data retention policies and applicable law;
- Personal Data must be kept secure;
- if applicable, data subjects must be informed of their legal rights; and
- principles of data protection by design and by default should be followed in designing a service or solution which Processes Personal Data.

International Data Transfer Annex

Fujitsu is committed to undertaking international transfer of Personal Data (both within the Fujitsu group of companies and externally) in a legally compliant way and more particularly in accordance with the steps set out below.

Step 1 – Controller Instructions

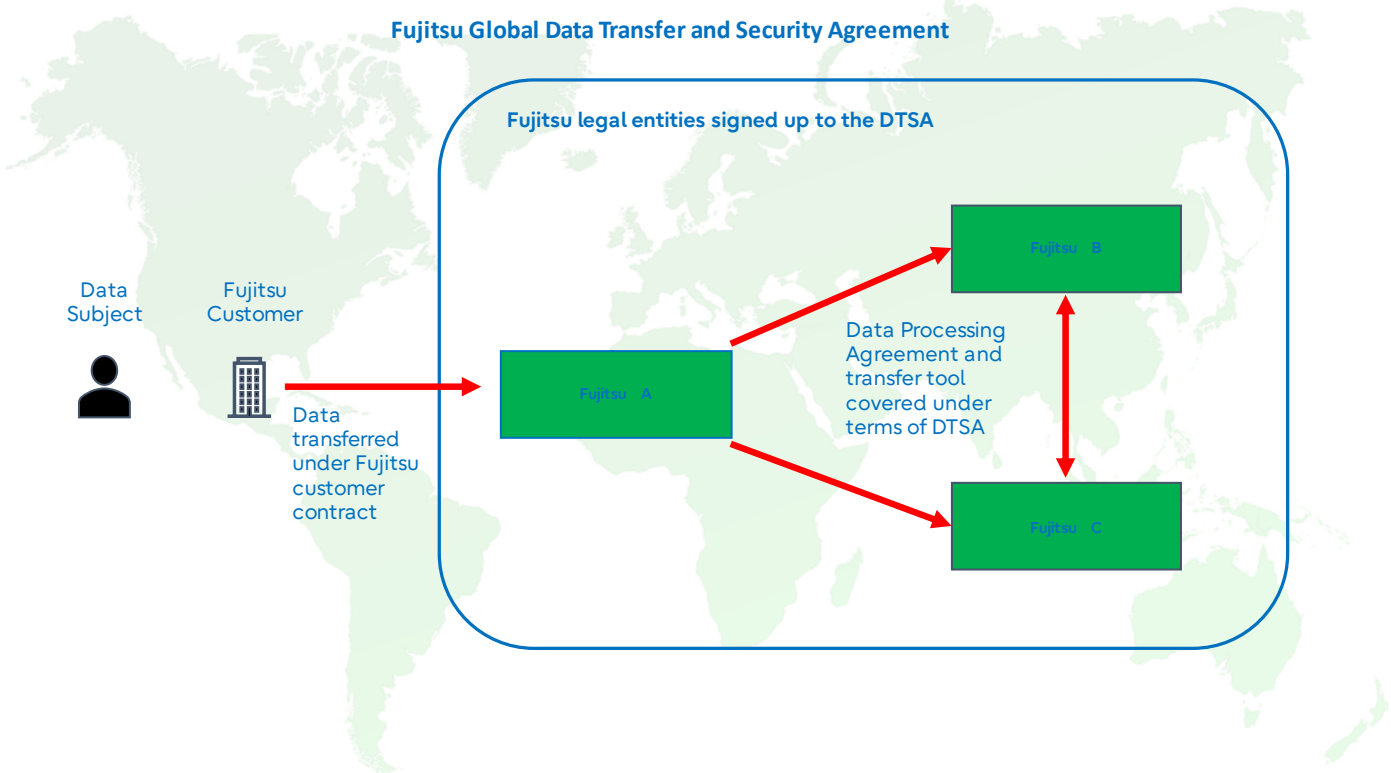
If Fujitsu is processing personal data on behalf of our customers, Fujitsu will ensure that it has the customer's prior approval, or instruction, to undertake a relevant transfer. This will usually be given in the data processing terms (or separate Data Processing Agreement, where relevant) of the contract between Fujitsu and the customer.

Step 2 – Contractual Terms

Fujitsu will ensure it has appropriate contractual terms in place between the Fujitsu legal entity transferring the data and the legal entity receiving the data. This will require both:

a) data processing terms; and
b) for transfers outside the EEA/UK to jurisdictions not in receipt of a valid adequacy decision (recognized under the applicable data protection legislation), appropriate data protection safeguards which meet the requirements of GDPR and/or UK GDPR Article 46.

For transfers between Fujitsu group entities, Fujitsu uses its Global Data Transfer and Security Agreement ("**DTSA**") to put in place the required data processing terms (in line with a) above) and the appropriate data protection safeguards (in line with b) above). The DTSA uses the latest standard contractual clauses approved by the European Commission ("**EU SCCs (Standard Contractual Clauses)**")") alongside the UK Information Commissioner's Office international data transfer addendum ("**UK Addendum**"), where required. All relevant Fujitsu entities are signatories to the DTSA.



For transfers by a Fujitsu entity to a third party supplier located in a jurisdiction not in receipt of a valid adequacy decision, Fujitsu will ensure that such transfer is undertaken in compliance with Chapter V of the GDPR and/or the UK GDPR, as applicable, and implements appropriate safeguards in accordance with Article 46 of the GDPR and/or the UK GDPR where legally required.

Step 3 – Transfer Impact Assessment

Fujitsu will also undertake transfer impact assessments ("TIAs"), where legally required, to evaluate whether the EU SCCs and UK addendum (or other applicable transfer tools) are effective in the circumstances of the transfer and assess whether supplementary measures are necessary to protect the Personal Data as a result of the transfer. Fujitsu undertakes this third step using a centralized approach and template.

Fujitsu can upon request provide details of the relevant transfer to support customers with their own transfer impact assessments. If any supplementary measures are identified by the customer, as data controller, to be appropriate to the relevant transfer, then such measures should be discussed and where agreed reflected within the contract between customer and Fujitsu.

