WHITE PAPER
TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES IN BASWARE SERVICES

INTRODUCTION

On 16 July 2020, the European Court of Justice ("**CJEU**") delivered its judgment in Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties (Case C-311/18) ("**Schrems II**"). According to this judgment, transfers of personal data from the European Economic Area ("**EEA**") to third countries under the application of the EU Standard Contractual Clauses ("**SCCs**") or other appropriate safeguards (listed in Article 46 GDPR), as a transfer mechanism, will be valid only if the data exporter can verify, on a case-by-case basis, that the **level of protection provided to the personal data following the transfer is essentially equivalent to and does not undermine the level of protection guaranteed to individuals under EU law / GDPR**.

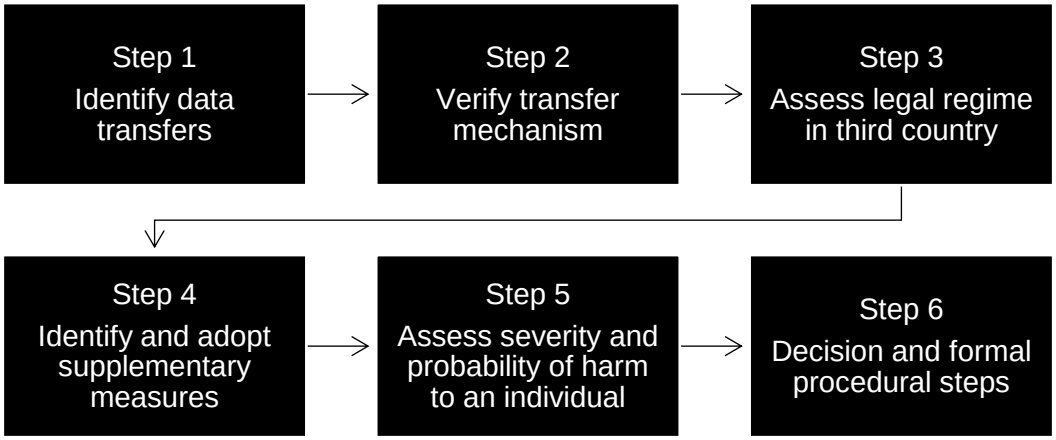
Such transfer assessment should on the one hand consider whether the underlying legal regime in the third country provides essentially equivalent protection to that afforded in the EU. On the other hand, the assessment should also look at supplementary measures which may mitigate potential shortfalls in the level of protection afforded in the related third country.

In response to the Schrems II judgment, the European Data Protection Board ("**EDPB**") has adopted recommendations to assist data exporters to identify and implement supplementary measures where needed to ensure the appropriate level of data protection.

Following the Schrems II judgment and the EDPB recommendations, Basware Corporation ("**Basware**") has created a **data transfer impact assessment methodology** in cooperation with global law firm DLA Piper in order to ensure continuous compliance with GDPR when transferring personal data from the EEA to third countries. The methodology provides required tools for Basware to assess safeguards when transferring personal data to third countries. It is fully aligned to the requirements of GDPR following Schrems II.

BASWARE'S METHODOLOGY FOR DATA TRANSFER IMPACT ASSESSMENTS

The methodology used by Basware to assess personal data transfers from the EEA to third countries involves a six-step process, including an embedded scoring model applied during steps 3 to 5.



Below is the summary of implementation measures taken by Basware based on the six-step process. More specifically, the summary demonstrates the measures taken by Basware to assess the transfers of customer personal data to third countries in connection with the provision of Basware's services.

SUMMARY OF BASWARE'S DATA TRANSFER IMPACT ASSESSMENTS

Step 1: Identify data transfers

All customer personal data transfers from the EEA to third countries in the context of Basware's services have been mapped with respect to the factual details of data flows associated with each transfer. Relevant data transfers, not subject to an adequacy decision from the EU Commission, in relation to customer personal data take place to the following third countries: Australia, India and the USA.

The transferred personal data concerns Basware customer's business related contact data (including username/password) of individuals involved in the usage of Basware's services and of individuals mentioned on business documents processed through Basware's services. By default, the data of Basware's EEA customers is processed through Basware's service applications hosted on servers located within the EEA. The specific transfers take place only where it is necessary for Basware's sub-processors to access the data in order to carry out operation, development, maintenance and support tasks. All access to personal data by third country sub-processors are incidental in nature. Furthermore, access to the personal data by Basware's sub-processors may take place only in accordance with the need-to-know principle.

Step 2: Verify transfer mechanism

SCCs are used as a mechanism to transfer Basware's customers' personal data to Australia, India and USA. Following the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Basware is in the process of implementing the modernized SCCs to cover each relevant transfer. Copies are published on www.basware.com/general-terms.

Step 3: Assess legal regime in third country

Basware, in cooperation with DLA Piper, has performed an assessment on the extent to which the legal framework in Australia, India and the USA respectively provide legal protections for personal data that are essentially equivalent to the guarantees offered within the EU. This part of the assessment involved consideration of the five key criteria[1] regarding the legal framework and as a result an inherent risk score was established for each third country.

Based on these assessments, Basware has identified the relevant areas of the third country legal frameworks that may impinge the effectiveness of the appropriate safeguards provided by the

[1] The five key criteria of the third country legal framework include an assessment on: regulation on the processing of personal data; regulation of public authority access to private data; regulatory supervision; rights of redress; and applicable international treaties.

SCCs. As a result, Basware has reviewed its existing and has implemented new supplementary technical and organizational measures.

Step 4: Identify and adopt supplementary measures

Taking into account the assessments in step 3, Basware confirms to have in place the following supplementary technical and organizational measures:

- Basware's services are protected using both network and logical level security solutions. Industry standard cloud security solutions are used as well as third party security products and services within the cloud service environment. Administrative access to the service environment requires separate authorization and use of dedicated administrative tooling.
- Basware's user accounts used to access and authorize access to the service applications are managed under Basware's responsibility using the principle of least privilege, which is based on access requirements of defined job roles.
- Access logs and actions are being stored for a reasonable period of time, based on criticality.
- Basware provides the services in co-operation with its hosting service provider. The hosting service provider defines and maintains the physical and environmental controls for production environments. The provider has assurance reports and security certifications covering these controls and additionally these controls are under regular scrutiny by Basware.
- Network traffic over public Internet is encrypted and customer data in storage is encrypted. Encryption key management is carried out with using industry best practices.
- Basware uses a dedicated encryption key management service under which:
    - Basware owns the encryption master keys in its Basware account.
    - Basware's master keys are created on FIPS 140-2 validated hardware security modules ("HSMs") which have physical security mechanisms to show evidence of tampering. These HSMs protect the confidentiality and integrity of Basware's master keys. The master keys never leave the above-mentioned HSM on which they were created, are never written to disk and are only ever used in the volatile memory of the HSMs for the time needed to perform the requested cryptographic operation.
    - Based on the design of the HSMs, no one, including personnel of the key management service provider, is able to retrieve Basware plaintext master keys from the HSMs or key management service.
    - The master keys relating to Basware's services to EEA customers are created on HSMs in the EEA and are not transmitted outside of the EEA.
- Basware maintains an internal policy for handling third party data access requests.
- Basware is discussing supplementary contractual safeguards with third country sub-processors in order to reinforce the safeguards that the SCCs provide.

Step 5: Assess severity and probability of harm to an individual

Basware has assessed the potential risk of harm to an individual arising from the transfers as well as the likelihood of that harm being occurred. The assessments indicate that the risk of harm to an individual resulting from third country public authority access to customer personal data would

be low. The transferred data does not include or reveal sensitive data or other particularly private data that could be used against an individual by third country public authorities.

In addition, Basware assesses the likelihood of third country public authorities requesting access to any customer (personal) data as low. No such requests have been received by Basware or its sub-processors so far. Basware assesses that its operations are of low interest to public authorities searching for data on individuals.

Step 6: Decision and formal procedural steps

Based on the assessments carried out, Basware is confident that the implemented supplementary technical and organisational measures mitigate the risk of public authorities' access to customer's personal data to an acceptable level.

The SCCs used as a transfer mechanism do not need an authorization from a competent data protection supervisory authority and thus no additional formal procedural steps are necessary.

Basware will conduct annual reviews on the data transfer impact assessments in order to ensure that any changes in the circumstances of the data transfers are taken into account. More frequent reviews will be performed as needed based on new legislation in a third country.

NOTE

Any questions about this White Paper or our data protection practices can be sent to the Basware Data Privacy Team at privacy@basware.com.

The White Paper shall be for informational purposes only and shall not create or constitute any legal or other obligations for Basware. It shall be updated in accordance with the progress of Basware's data protection compliance program and the information contained herein shall therefore only apply for a limited period of time.

We trust that this White Paper sufficiently informs our customers on the related topic.

Kind regards

Basware