Transfer Impact Assessment Process FAQs

General Questions

Question	Answer
Why the change?	An EU judgment in July 2020 ('Schrems II') made EU/UK data protection laws stricter on transferring EEA/UK origin personal data outside of the EEA/UK. Essentially it changes the way that we need to interpret the GDPR. To comply with the GDPR after Schrems II, all procurement and business teams dealing with a third-party supplier will have to carry out risk assessments and put additional contractual, operational, and technical measures in place to protect EEA/UK origin personal data, for both external and intra-group data transfers while continuing with our organisation's business activities.
What are the benefits of complying with the GDPR?	Avoiding fines of up to 4% group global turnover or 20 million Euros (whichever is higher), claims from affected individuals / privacy activist groups and damage to QBE's reputation and ultimately Group share price. To comply with QBE's obligation a Data Transfer Impact Assessment Process has been developed that helps the organisation identify and mitigate the risks involved with Data transfers outside the European Economic Area ("EEA") and or the United Kingdom ("UK"). We also receive requests from our business partners, who seek our assurance that QBE are compliant before they continue to share data with us. This includes key brokers, government agencies, reinsurers, and Policyholders. Carrying out Transfer Impact Assessments is just a new cost of doing business.
When is this happening?	We have been piloting the new process with several procurement teams during Q4 2022. Business engagement will commence in February 2023, with a planned cutover to the new process on 6 March 2023 for all new engagements with suppliers, and a staggered implementation for supplier contract renewals.
Who does this change affect?	This process is only relevant when personal data originating in the European Economic Area (EEA) or United Kingdom (UK) is transferred anywhere outside of the EEA, the UK and/or any country considered 'Adequate' by the European Commission (including hosting and remote access). The change impacts all procurement and business teams within European Operations that contract with third party suppliers. They will now have to perform a Transfer Impact Assessment to assess and mitigate the risk of possible data transfers to a country outside the approved list.

'Adequate' (i.e. approved) countries	The following 'Adequate' countries provide an 'essentially equivalent' level of data protection to that which exists within the EU: Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea (South Korea), Switzerland and Uruguay.
High Risk Countries	There is no official list of countries which are 'high risk'. However, the QBE project team takes the view based on various data sources that sending personal data to the following countries may involve higher risks for individuals' privacy and/or human rights: Afghanistan, Algeria, Belarus, Burundi, Cameroon, Central African Republic, Chad, The People's Republic of China, Colombia, Crimea (Region of Ukraine), Cuba, Democratic Republic of Korea (North Korea), Democratic Republic of the Congo, Egypt, El Salvador, Eritrea, Haiti, Honduras, Hong Kong, Iran, Iraq, Israel (West Bank and Gaza only), Kenya, Lebanon, Libya, Mali, Mauritania, Mexico, Niger, Nigeria, Pakistan, Russia, Saudi Arabia, Somalia, Republic of South Sudan, Sudan, Syria, Thailand, Ukraine, Venezuela, Yemen, Zimbabwe. A transfer to a country not on this list (such as the United States of America) could still be 'high risk' depending on the circumstances of the transfer. If a country is not on the 'Adequate' list, and personal data which is not 'low risk' are being transferred, an assessment must be completed.
How does the process work?	There are two parts to the Transfer Impact Assessment process: • An initial Screening Transfer Impact Assessment asks questions to identify the type of personal data that will be in scope of the 'arrangement' (EO or Group contract or business process), the location of the data subjects that the personal data relates to and whether it involves the movement of, or access to, personal data across international borders. The answers to these will dictate whether the additional assessment needs to be completed. • Depending on the answers (for example if there are international transfers of any personal data which is not 'low risk' personal data), a second more detailed assessment (Full Transfer Impact Assessment) will have to be completed. The assessment will focus on identifying the entities involved, business activities and data in scope, countries involved, if there are onward transfers by the supplier, and understand if risk mitigation controls are (or can be put) in place (either technical, organisational, or contractual controls)

One Trust Tool Questions

How do I access the OneTrust Portal?	Please use the following link https://qbe.my.onetrust.com/assessment/wizard/select
Which assessment form should I open first?	Please launch the Screening Assessment form first. Please launch the most recent version of the Screening Assessment form first. See the user guide for more information.
What is classified as sensitive personal data?	Sensitive personal data is information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation, criminal convictions, and proceedings. For example: • Medical records/ health information • Ethnicity/ Religion/ trade union/ political/ sexual orientation • Police criminal record checks • Facial recognition data (or other biometric/ genetic data) • Claim descriptions that include health information • Personal data of vulnerable persons (e.g. children or persons lacking mental capacity) • Social security number of individuals based in France • Free text fields (risk may contain sensitive personal data)
What is classified as 'low risk' personal data for the purposes of the QBE Transfer Impact Assessment process?	'Low risk' personal data in this context is **only** personal data as described below, and no other data. Low risk data includes: - Name - Company email address - Company telephone - Country or region location (e.g. UK / EMEA) - High level public information about a job role or job activities (e.g. job title, non-confidential information about activities carried out on behalf of employer) - Employee ID - Basic login details for a system used by QBE employees, customers or commercial partners in the course of carrying out activities business activities Some examples of personal data that would **not** fall within this definition, although this list is not exhaustive, are: personal addresses; medical data; ethnicity; religion and sexual orientation.
Does the system have any alerts or notifications?	Yes. The system will: • Notify the **respondents** that they have an assessment to complete • Notify the **approver** when the respondents have submitted the assessment • Notify the **approver** when the assessment has been reviewed by the Data Protection Team In order to receive these notifications, the **creator** needs to assign themselves as an '**approver**'. Do not forget to always include Stuart Skippings (DP Team) as an approver.

Does the system have reminders?	Yes, the system will send weekly reminders to the respondents until they submit the assessment and cannot be switched off.
Do I need to answer all questions?	To submit the assessment, you need to answer at least all the mandatory questions (those marked with a red asterisks). The system has been designed to only ask relevant questions based on previous answers.
Can I attach documents?	Yes, you can attach documents using the paper clip button. Any attachments over 250mb will need to be sent to the DP inbox with the name of the assessment they relate to. 
Would a supplier also receive an assessment result?	Yes – the supplier will be told whether the assessment has been approved but would not receive any comments that have been added by the DP Team when completing the review. Approvers will also receive the assessment result.
What are the reassessment criteria?	At contract renewal but where Evergreen applies it should be a maximum term of 3 years before reviewing again. Some high-risk arrangements may be required to be reviewed more frequently.
Who should suppliers contact if they need support?	Suppliers should contact DPO@uk.qbe.com for support.