Insight's Response to *Schrems II* on Cross-Border Data Flows

As you may be aware, on July 16, 2020, the European Court of Justice made a key data protection ruling in what is now commonly referred to as Schrems II. In its decision the court made two principle findings. Firstly, the court invalidated Privacy Shield as a legitimate data transfer tool. Secondly, the court validated Standard Contractual Clauses (SCCs) as a legitimate transfer tool and introduced some additional considerations for data exporters and importers of personal data subject to SCCs. This decision has significant implications for organisations.

For several years Insight has provided clients with overlapping and complimentary protections under both SCCs and Privacy Shield frameworks for data transfers. While Insight currently continues to maintain its Privacy Shield certification, it does not rely upon it. From the point of invalidation by the court, any export within the Insight Group of covered clients' data outside of the European Union or EEA is under the continued protection of SCCs.

Supply chain screening

In compliance with the court's decision, Insight does not accept Privacy Shield within our supply chain as a lawful transfer tool for transfers of covered client data outside of the European Union or EEA. In order to protect client data Insight insists that suppliers process data on protective contract terms and where data is transferred out of region under one of the compliant transfer tools under Article 46 GDPR (for example SCCs or Binding Corporate Rules (BCRs)). Insight employs screening processes to obtain assurances around the data protection compliance practices including data transfer mechanisms within our supply chain. As a matter of standard practice Insight uses SCCs as the relevant data transfer mechanism with our suppliers.

Initial Schrems II Assessment and Roadmap

In line with the court's decision in Schrems II and applicable regulatory guidance, Insight is taking the necessary measures to ensure our ongoing compliance and a level of protection for client data which is essentially equivalent to the EU standard. In so doing we are in the process of following the six steps roadmap contained in the recently adopted European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools and we are closely monitoring further guidance. Insight places utmost importance on privacy and security and remains committed to maintaining high levels of privacy and security in respect of our partner and client data.

EU (inc. EEA)/UK Data Transfers Following Brexit

The EU and the UK have mutually recognised each other's data protection standards as offering "data adequacy" with both countries having an essentially equivalent level of protection. This means that personal data can continue to flow freely between the EU (including the wider EEA block) and the UK, without the requirement of entering into appropriate safeguards (e.g., Standard Contractual Clauses).

Summary of personal data that Insight processes

The exact categories of client personal data that Insight processes will depend on the products and services that we supply to you. In most cases, Insight will process only limited amounts of (non-sensitive) client personal data. For normal transactional business (being the provisioning and supply of standard third-party products and services), the data will usually be limited to normal business contact information such as names, and business email addresses and delivery addresses. We would only request the minimum amount of data necessary to receive, fulfil and deliver client orders, and for normal account management and reporting purposes (where required).

In the context of consultancy, managed or other professional IT services the processing will be focused on the fulfilment of the services engagement. Ordinarily there will be a statement of work or similar document which details the specific services which will explain the type of data processing activities required. Insight does not sell, rent or trade partner or client personal data.

cont/

Insight's Response to *Schrems II* on Cross-Border Data Flows

A Global IT Organisation – Data Residency

We recognise that the residency or location of personal data is important for many clients. Despite being part of a U.S. headquartered organisation, our EMEA business maintains a separate instance of many of our main IT systems on data centers located in the UK/Europe. Wherever practicable we will use "multi-geo" systems to keep data within a particular country or local region.

There is a small minority of client personal data which is processed outside Europe. However, such data is mostly limited to reporting for global clients and is ordinarily restricted to the basic business contact information of those individuals involved in receiving our services. Any such processing is in line with any contractual arrangements we have with particular clients, and would be covered by the transfer tools we have in place to effect such transfers as discussed above.

Information Security

Insight recognises that Information security and the governance of data are important elements of the GDPR. Insight implements encryption in transit and encryption at rest to secure and protect its partner and client data.

We understand that the confidentiality, integrity and availability of the information entrusted to Insight by its partners and clients is vital. Insight maintains a formal global Information security program that is compliant with legal and regulatory requirements, as well as our contractual obligations, relevant to ensure that all the data we hold is safe and secure. We enable policies, procedures and technical controls to see that the full lifecycle of data is safely maintained.

FISA 702 and EO 12333

Based on our understanding of the law and its definitions, and given the nature of services provided by Insight to its customers, it is Insight's opinion that Insight is not an "electronic communications services provider" subject to FISA 702, and Insight has never been told otherwise by any regulatory body or U.S. intelligence agency. Furthermore, Insight has never received an order to disclose its data or its customers' data under FISA 702, nor has Insight ever otherwise provided European personal data belonging to its customers subject to GDPR to any U.S. intelligence agency. Furthermore, Insight has never received any request for any of Insight's customer data by any U.S. intelligence agency pursuant to EO 12333, nor is Insight aware of any action relating to or access to any of Insight's customer data by any U.S. intelligence agency pursuant to EO 12333.

MKT4543 UPDATE