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.

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)).

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.

Brexit

Negotiations are ongoing between the EU and the UK on a future trading relationship including transfers of data. No matter what the relationship will be on 1 January 2021, Insight will ensure it has an effective and lawful framework in place to ensure the ongoing flow of data between the UK and the EU. For our UK based clients this will mean, amongst other things, ensuring compliance with the UK data protection regime and the free flow of data back into the UK of any EU based data assets, and vice versa for our EU clients.

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.

A Global IT Organization – Data Residency

We recognize that the residency or location of personal data is important for many clients. Despite being part of a U.S. headquartered organization, 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 recognizes that Information security and the governance of data are important elements of the GDPR.

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.

MKT4543