OUR PROCESSING AGREEMENT

*This fact sheet is part of Crayon's proactive communications strategy on **Information Security and Data Protection (ISDP)**.*

Crayon, our Customers and Suppliers, all have an obligation under the European Union (EU) General Data Protection Regulation (GDPR) to safeguard the rights of the individuals whose Personal Data we process. To ensure our Business to Business (B2B) processing relationships are built on the foundations of GDPR compliance we must satisfy two mandatory obligations:

- The use of a Supplier (i.e. a 'Processor') to process Personal Data on your behalf must be '**governed by a contract**' such as a **Personal Data Processing Agreement (PDPA)** which includes your company's rights and obligations as the Customer (i.e. the 'Controller'), and covers those data categories required under Article 28 GDPR.
- Each 'Controller' and 'Processor' must '**maintain a record of processing activities** under its responsibility'. And we invite our Customers and Supplier to use Crayon's PDPA Annex as it covers the data categories both require under Article 30 GDPR.

This fact sheet describes the rationale and design process behind the **PDPA + Annex** Crayon offers to our Customers and Suppliers to ensure our processing relationship is GDPR compliant and all parties have the data they need for smart compliance management – i.e., critical data is on-hand so you can efficiently and effectively manage a data breach, audit, or a subject access request (SAR) from individual who wish to exercise their rights under the GDPR.

In general, PDPAs are often completed by operational employees who procure/deliver services to support core business activities. While we train these employees so they know how to securely process data and protect the rights of data subjects, they lack the legal expertise to assess the PDPAs they are asked to sign-off. Accordingly, this fact sheet also explores the GDPR's legal obligations and practical compliance challenges so that operational employees can take informed decisions when confronted with a PDPA.

LESSONS LEARNED

From our own compliance journey, we learned that **organisations must implement smart tactical solutions in each compliance vector if they want to succeed in managing the complete portfolio of GDPR requirements**. Our solution for B2B processing relationships is based on the following analytical findings:

- **The combination of 'PDPA + Annex' can provide both Processors and Controllers with robust processing safeguards** (e.g. if the implementation of technical security measures is documented in relation to explicit data transfer/access scenarios) and **significantly reduce their secondary compliance costs** (e.g. if it covers key data points required for SARs and audits).
- **Annexes that cover the data points referred to in Articles 28/30** GDPR can provide a transparent separation of each party's **processing responsibilities** (e.g. for technical security depending on if data is transferred to, or just accessed by, the Processor).
- **Using Annexes to map accountabilities on the operational level** provides both parties with a clear overview of their ongoing **compliance management requirements** and the assurance to adopt a **balanced approach to liability in the PDPA itself**.
- **Attempting to deflect liability through a PDPA is risky and unnecessary.** Controllers are assigned with the principal liability for damages caused by processing which infringes the GDPR; liability which can be claimed back from the Processor to the extent that the Processor is liable. However, some PDPAs try to deflect liabilities onto the Processor. While this strategy may backfire as it may contradict the GDPR itself, it will remain a point of contention before it is tested in court.
- **Adopting a 'lift + shift' approach to the completion/management of processing records is risky and short-sighted**. Some PDPAs state that the Processor shall be responsible for record keeping on behalf of the Controller. While this strategy may reduce the initial cost of record creation for the Controllers, these savings can rapidly be outweighed by the cost of obtaining records (that may not exist) from Processors in the event of an audit. In addition, if these Controllers do not have a robust alternative to demonstrate they perform adequate due diligence, they must be prepared to receive substantial fines.

SMART SOLUTION

At Crayon, **we took the tactical decision to offer our Customers/Suppliers a balanced and mutually beneficial PDPA** – one that we would be prepared to use both when we act as the Processor and when we are the Controller. We then analysed the legal and practical challenges of our various stakeholders in managing their ongoing GDPR compliance requirements to design a smart solution that enables the businesses we work with to:

- **Save thousands of Euros on legal reviews** by adopting a balanced PDPA that is grounded in the principle of shared interest and ownership between Controllers and Processors to protect Personal Data and safeguard the rights of data subjects.
- **Decrease B2B processing risks** by completing a PDPA + Annex which provides a wide range of data points required for a robust and lean risk management model.
- **Focus on the negotiation of the delivery of services that meet core business needs** instead of GDPR-related disputes.
- **Reduce the risk of inaccurate and incomplete records** by using the same PDPA + Annex for both Customers and Suppliers.

*For more information on Crayon's GDPR compliance model or a copy of our PDPA template, please contact: **dpo@crayon.com***