Data Processing Policy
APTECH SYSTEMS LIMITED

May 2018

1. Purpose and scope of Aptech systems Ltd Data Processing on behalf of Data Controllers

For the purpose of providing the Services, Aptech systems Ltd will process Customer Hosted Data. To the extent that Customer Hosted Data is comprised of Personal Data, the parties acknowledge that Aptech systems Ltd acts as a Data Processor for all Customer Hosted Data supplied to Aptech systems Ltd by the Customer as well as the Customer's own customers or agents.

The Services are provided on the basis that either:

the Customer is the Data Controller for all Customer Hosted Data supplied to Aptech systems Ltd under the Services and has complied with its obligations under the applicable Data Protection Laws, including but not limited to obtaining the required consents ("Data Protection Consents"); or

where the Customer is a Data Processor on behalf of a Data Controller, that Aptech systems Ltd is a sub-Data Processor and that the Customer has:

- ensured that all necessary Data Protection Consents have been obtained or other lawful grounds for Processing have been correctly established;
- entered into the required contractual arrangements, including arrangements with the relevant Data Controller for Aptech systems Ltd to act as sub-processor legally;
- has complied with its obligations as Data Processor under the applicable Data Protection Laws; and
- shall be liable to the Data Controller for Aptech systems Ltd's acts and omissions and a sub-Data Processor.

By accepting this ASL's Data Processing Policy, the Customer indicates their acceptance of the provisions below and warrants that the basis of the Services set out in this Data Processing Policy is accurate.

2. Nature of the Processing

Aptech systems Ltd undertakes a range of Processing as defined by the Services, i.e. the provision of application or server hosting services to the Customer, the choice of which is determined by the Customer. The Customer acknowledges that the scope of the Services explicitly excludes the access to, manipulation, transformation or optimisation of or decision-making based on Customer Hosted Data for the purposes of such Processing by Aptech systems Ltd. ASL provides a dedicated and cloud-based application or server hosting infrastructure to support the Customer's or Customer's agents' processing of data to that end.

Aptech systems Ltd has no intention to access or manipulate Customer Hosted Data, even in the case where Aptech systems Ltd maintains technical access for the purposes of management of the infrastructure of the Customer Hosted Solution. This is due to the Customer's position as the Primary System Administrator. Aptech systems Ltd interacts with the Customer Hosted Solution for the purpose of management and support only. Further, any processing by Aptech systems Ltd of Customer Hosted Data (which may comprise Processing of Personal Data) is determined by the Customer insofar as it is the Customer that ultimately determines what the Services will be and, therefore, what data processing occurs.

Aptech systems Ltd classifies all Customer Hosted Data as the same type of data and does not maintain visibility of different types or Customer Hosted Data or categories of Personal Data within this set. Aptech systems Ltd applies the same level of generic security controls to all Customer Hosted Solutions.

Aptech systems Ltd provides a service which constitutes among other things the provision of VMs, storage, networking and dedicated servers to Customers. Whilst we will try to ensure the compliance of those underlying services with the applicable Data Protection Laws, we do not maintain reliable

access to data that Customers upload to their Customer Hosted Solution, so the Customer is responsible for all data protection issues not related to the underlying services.

3. Duration of Processing

The Customer is responsible for the duration of the processing of any Personal Data comprising Customer Hosted Data. While the Agreement is in force, Aptech systems Ltd will Process all such Personal Data in accordance with the Customer's written instructions.

4. Aptech systems Ltd Responsibilities

SECURITY AND COMPLIANCE OF THE UNDERLYING HOSTING APPLICATION AND INFRASTRUCTURE

Aptech systems Ltd will be responsible for maintaining the GDPR compliance of the underlying hosting infrastructure, Aptech systems Ltd support personnel (including that such personnel are subject to a duty of confidence that is compliant with the applicable Data Protection Laws) and physical locations, including appropriate technical and organisational controls to secure and ensure the resilience of the underlying hosting application and infrastructure as defined by our hosting provider in their ISO27001 security procedures.
Aptech systems Ltd has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures. A non-exhaustive list of technical and organisational measures are as set out below. By entering into this Data Processing Policy, the Customer confirms that it has reviewed and approved the following measures:

a) SECURITY MANAGEMENT & POLICY

Maintenance of applications and an overarching information security management system Security and Compliance teams to help ensure Aptech systems Ltd operational and policy/audit security matters receive appropriate attention and resourcing, including Operations Board seats for both department representatives respectively

b) HR & ACCESS CONTROL

Vetting of all Aptech systems Ltd personnel prior to commencement of employment Appropriate on-hire, role change and termination activities related to Aptech systems Ltd access and asset management

Use of a role-based access control system and restriction of all Aptech systems Ltd access to customer data or Customer Hosted Solutions to those personnel with a business need for access

c) PHYSICAL & ENVIRONMENTAL SECURITY

Sufficient physical and environmental security controls at all Aptech systems Ltd facilities

d) OPERATIONAL SECURITY

Appropriate availability, performance and security logging, monitoring and audit controls for the underlying applications

Vulnerability management systems to help ensure the patch and configuration levels of the underlying applications appropriate to Aptech systems Ltd's scale and policies

Hardening of underlying infrastructure devices to levels that are materially in accordance with good industry practice

Backups and infrastructure redundancy within the underlying hosting applications and infrastructure appropriate to our Terms and Conditions and client SLAs

Appropriate security of all Aptech systems Ltd end-user devices used by Aptech systems Ltd to access the underlying hosting applications and infrastructure, Customer Hosted Data and Customer Hosted Solutions

e) INCIDENT MANAGEMENT & COMMUNICATION

Sufficient internal incident management procedures including the commitment to escalate relevant security incident to impacted Customers without undue delay

f) AVAILABILITY OF CUSTOMER HOSTED SOLUTIONS AND SERVICES

Temporary loss of Availability or Integrity related to an Emergency Maintenance or Scheduled Maintenance is not considered to be a loss of Availability under the applicable Data Protection Laws.

As set out in customer SLAs, Aptech systems Ltd guarantees the availability of applications and data centre services, e.g. availability of core network connection, power and cooling, and the availability of sufficient hypervisor capacity where Cloud services are procured in line with the provisions of the services' respective SLAs and Aptech systems Ltd's definition of Availability. In accordance with the Services being provided, Aptech systems Ltd is not able to decide how Personal Data comprising Customer Hosted Data is uploaded or processed by clients or sub clients. The Customer Hosted Solutions are inevitably software-as-a-Service-based and control of the data thereon is with the Customer.

5. Customer data protection responsibilities

As the application Administrator and / or Data Controller the Customer has the following responsibilities under GDPR:

1. Maintain appropriate customer access controls on customer applications to secure and monitor for security:

   I. the Applications

   II. Monitoring of the Customer staff and user access to the Hosted Solution for signs of security incident or intrusion

   III. all non-Aptech systems Ltd user access

   IV. Ongoing management of any anti-malware controls residing on Customer machines or customer infrastructure

2. Where the above is included within the scope of a Customer SLA, Aptech systems Ltd will undertake the work based on instructions from the Customer in ticket form, but the Customer remains responsible for the efficacy of the controls implemented.

3. Undertaking all organisational measures required to ensure compliance with the basic principles for processing (articles 5, 6, 7 and 9 of the GDPR) and Subject's rights (Articles 12-22 of the GDPR) at point of collection of data, and be aware of the technical and organisational security controls put in place by Aptech systems Ltd, maintain additional technical and organisational controls to ensure compliance during processing, storage, any transfer not undertaken solely by Aptech systems Ltd and at point of destruction, if not reliant on Aptech systems Ltd's underlying solution-level data destruction processes. (I.e. deletion of a data base or decommissioning of a dedicated server and associated storage media.)

4. Undertake and manage all communication with Data Subjects

5. Maintain any required relationship with the Information Commissioner's Office on behalf of the Data Controller

6. Aptech systems Ltd use of Data Sub-Processors

By entering into this Data Processing Policy, the Customer hereby permits Aptech systems Ltd to appoint sub-processors of Personal Data and, for the term that the Data Processing Policy is in force, shall have a general right to appoint sub-processors of Personal Data. Aptech systems Ltd shall provide the Customer with prior notification before appointing any sub-processors of any Personal Data that are in addition to those noted in this Data Processing Policy.

Aptech systems Ltd utilises a small number of Data Sub-Processors in order to provide Services to the Customer. The following list of Data Sub Processors used to provide Services will be updated from time to time to reflect the current operational position:

Memset Ltd – Provision of Colocation hosting and 1st line data centre remote hands support

Microsoft Ltd – Provision of Aptech systems Ltd email used for communications with the customer

Sage.com Sage Ltd – Provision of Aptech systems Ltd sales and account management systems

ACT.com ACT Ltd – Provision of contract management

Aptech systems Ltd will update the Customer of the use of any new Data Sub-Processor at least one (1) month prior to adoption of the Sub-Processor and transfer of Customer Hosted Data or provision of any form of access to Customer Hosted Solutions by support ticket or email, and the Customer must ensure that all necessary Data Protection Consents are obtained or other legitimate grounds for processing the Personal Data are established. The Customer's continued use of the Services constitutes approval for the use of this new Data Sub-Processor and a repeated warranty by the Customer that the use of all sub-processors is lawful under the applicable Data Protection Laws subject to Aptech systems Ltd complying with its obligations under the applicable Data Protection Laws in respect of appointing sub-processors. Aptech systems Ltd will perform appropriate due diligence on the Data Sub-Processor, as we will on any security-impacting supplier.

Aptech systems Ltd will maintain written contracts with all Aptech systems Ltd Sub-Processors including any relevant GDPR-related compliance requirements and will conduct regular audits to confirm their continuing conformance with Data Protection Laws.

7. Transfer to non GDPR-aligned locations or Sub-Processors

Aptech systems Ltd will not transfer Customer Hosted Data to any Data Sub-Processor located outside of the EEA or to any other third party location not deemed appropriate by Binding Corporate Rules, Privacy Shield or other adequacy decision defined on a continuing basis by the Information Commissioner's Office without explicit written permission from the Customer.

8. Processing in accordance with written instructions

Aptech systems Ltd will only processing Customer Hosted Data (which may or may not include data for which the Customer is the Data Controller) in accordance with the Data Controller's written instructions, which for the purposes of data protection and this policy are taken to be in whole contained within the section 'Purpose and scope of Aptech systems Ltd Data Processing on behalf of Data Controllers.' No other written instructions can be accepted as they will fall outside of the scope of our services.

9. Assistance with Customer data protection obligations

Insofar as Aptech systems Ltd provides a hosted applications and infrastructure to the Customer, Aptech systems Ltd will assist the Data Controller in meeting their data protection obligations including:

1. Provide the Customer with five (5) working day per annum in which they may undertake an onsite security and compliance audit of Aptech systems Ltd's services and premises. This must be scheduled and agreed with ASL Security and Compliance at least ten (15) working days in advance, including agreement of a detailed agenda for the audit. We are able to support audits performed by suitably empowered third parties on behalf of the Customer, but request that a Customer representative is in attendance in this case.

    a) Further audits as required by the Customer's compliance regime or in the event of an investigation will be charged on a reasonable time and materials basis, unless Aptech systems Ltd has reasonable evidence to suggest that the investigation is related to a material failure or weakness in our Services.

2. Maintain an up to date 'Data Protection Compliance' policy and documents available via the Aptech systems Ltd website that includes a range of policy information.

3. Carry out internal Data Privacy Impact Assessments as the Data Processor for all Services and to assist the Customer with consulting with the Information Commissioner's Office where these indicate an unmitigated high risk.

4. To inform the Customer of the possibility of a material security breach of their Customer Hosted Solution if detected by our systems without undue delay.

5. Provision of Customer admin access to the Customer Hosted Solution at point of initial deployment. (This constitutes the technologically possible extent to which Aptech systems Ltd can provide regarding Subject Access Requests regarding data for which the Customer or Customer's customer is the Data Controller.).

6. Keep a record of all Processing of Personal Data performed in relation to the Services.

7. Where a Security Incident resulting in a data breach has occurred or has been suspected to have occurred as a result of a material failure or weakness in the Aptech systems Ltd applications or infrastructure we will notify the Information Commissioner's Office and impacted Customers without undue delay

8. For termination of contract for reasons other than breach of Acceptable Use Policy or non-payment of fees, provide a reasonable period in which the Customer can use standard tools to extract the data themselves provided that such extraction by the Customer does not prejudice Aptech systems Ltd or its systems. In all cases Aptech systems Ltd will delete all Customer Hosted Data on our infrastructure as part of decommissioning of the Customer Hosted Solution.

9. Aptech systems Ltd shall assist the Customer in complying with its obligations under applicable Data Protection Laws in particular in relation implementing appropriate security measures, to carrying out a data protection impact assessment, and to consulting the competent data protection authority.