Privacy Compliance Statement

As one of the largest global software providers, our business depends on the continued provision of secure, reliable and compliant services that protect customer data and promotes customer trust. This statement should assure you that we take our data protection and privacy obligations – legal, contractual and operational – very seriously, and are actively working towards maintaining our continued compliance.

Additionally, we are committed to using data responsibly in order to uphold the rights of the individuals, and supporting the organizations with whom we work. Using data responsibly is not just an issue of technical security and encryption, but also of safeguarding the rights of people, ensuring their dignity, respect and privacy, and allowing them to make informed decisions when providing data.

Corporate responsibility

Data protection and privacy compliance is driven by our Privacy and Compliance Team at Micro Focus, and is supported by technical and legal subject matter experts, with executive oversight, including Board members. Data protection compliance is built into our corporate-wide information security management system, and is kept under review to ensure the required standards are met.

Compliance with current data protection and privacy laws

We have a regime in place to ensure we maintain our compliance with data protection requirements imposed by data protection and privacy laws (when we act as a Controller) and by contract (when we act as a Processor on behalf of our customers).

Insight into our compliance achievements

The following are examples of our current practices and procedures:

1. **Information security and Quality Management**
   We have implemented industry standard technical and organisational measures across our network of processing locations to safeguard our customers' data and we hold ISO27001 and ISO9001 certifications.

2. **Encryption**
   All corporate and end points feature encryption. We also apply encryption at rest.

3. **Checks and audits**
   We conduct periodic checks of our processing facilities and systems to ensure our security measures are aligned with our legal, contractual and certification obligations. These assessments are conducted by our Internal Audit function in association with PWC. Such audits include a full review of our policy and procedure documents that align with privacy laws and information security standards.

4. **Incident response**
   We have a robust data breach management system in place to ensure that, in the unlikely event of an issue that may affect our customers' data, it is promptly identified, notified to the customer and where appropriate to the regulator, and an effective investigation and remediation plan is quickly put in place.

5. **Training**
   All staff are trained on the secure handling, processing and use of personal data. This is part of our overall commitment to keeping data secure and minimizing any potential for human error.

6. **International data transfers**
   Where appropriate we enter into Standard Contractual Clauses with our customers where this is necessary for the transfer of data out of the European Economic Area and the UK (in line with Schrems II requirements). We flow these Standard Contractual Clauses down to relevant business partners and suppliers to ensure consistency of processing and the continued protection of data.

7. **Supplier management**
   We follow a comprehensive due diligence process when selecting relevant suppliers and business partners, using strict criteria that includes carrying out checks of their data protection and privacy processes, procedures and information security measures.

8. **Privacy by design**
   We apply privacy-by-design principles in the development and implementation of our products. We are therefore, very familiar with the importance of building privacy compliance into our data processing products and services. Our development teams work closely with the Product Security Team and the Privacy and Compliance Team to ensure appropriate expertise is included in the development process. Additionally, Data Protection Impact Assessments are carried out on all new system acquisitions and process changes.

9. **Registration with Data Protection and Privacy Authorities**
   Where appropriate we are registered with country-specific data protection and privacy regulators, and the registrations are reviewed and maintained by the Micro Focus Privacy and Compliance Team.

10. **Special note for regulatory compliance in China**
    Consultations on the second drafts of both the Draft PIPL and the Draft DSL were open until late May 2021. As a result, Micro Focus are monitoring the situation in China to ensure that a program of compliance is onboarded as soon as the new laws are introduced.

Privacy and compliance management

We understand the importance of reassuring our customers that personal data is safe with Micro Focus, for this reason, we have personnel within our Privacy and Compliance Team who are responsible for data protection and privacy compliance along with the support of internal and external advisors whenever necessary.

Kind Regards,

Micro Focus Privacy Office