Nuance Statement on GDPR

Nuance takes data protection very seriously. Our systems have been designed with features to assist organisations in safeguarding personal data, as defined in GDPR, such as providing organisations ways to secure prints, scans and copies when using the appropriate Nuance products.

When an organisation uses Nuance imaging products, Nuance is neither a Data Controller nor a Data Processor as defined in GDPR because Nuance does not have access to the organisation’s company directories or other personal data. However, advanced logging and administrative capabilities of solutions such as Nuance AutoStore combined with other Nuance Imaging products, in connection with the support provided by the solution provider, may assist organisations in meeting their obligations under GDPR, whether as a Data Controller or Data Processor.

As part of a broader system of organisational and technical measures which every Data Controller and Data Processor must adopt, Nuance can confirm that with Nuance AutoStore, organisations will have the tools to enable them to restrict access to devices to approved users only. Additionally, the organisation can track each user’s activities, creating a compliant audit trail for monitoring all input and output from the devices using AutoStore.

Nuance AutoStore, when deployed together with Nuance’s print management solutions, enable organisations to protect prints and scans by securing access to the device through authentication, where only users approved by the organisation can use the multifunction device (MFD) or networked print devices. The authentication process uses the organisation’s company directory (typically Active Directory or other LDAP-compliant solution), which should only be accessed and administered by the organisation’s authorized personnel to validate the user’s identity to match that of the company directory. Only upon a confirmed match is the user able to access Nuance print management or capture functionality on the device.

Scanned, uploaded and acquired documents, which might contain PID, are either temporarily stored in Nuance AutoStore, until they can be routed to destination systems (which are controlled by the organisation), or Nuance AutoStore administrators are enabled to remove and delete these documents according to business process requirements applying built-in tools. Document retention policies can be defined by a Nuance AutoStore administrator to remove any document which may have remained in the system as the result of a routing failure.