MJ FLOOD STATEMENT ON GDPR

MJ Flood takes protection of customer data very seriously. Our systems have been designed to safeguard personally identifiable data and provide organizations with ways to secure print, scans and copies when using SafeQ software.

SafeQ begins with ensuring that an organisation's prints and scans are protected by securing access to the device through authentication, by means of staff ID card or Personal Identification Number (PIN), where only approved users can use the multifunction device (MFD) or networked device within the SafeQ system. The authentication process uses the organisation's company directory (typically Active Directory or other LDAP-compliant solution), which is accessed and administered by the organisation's authorised personnel; it validates the user's identity to match that of the company directory. Only upon a confirmed match is the user able to access SafeQ on the device.

With SafeQ software and individual components, MJ Flood is neither a Data Controller nor a Data Processor as defined in GDPR, nor does it have access to an organisation's company directories. However, advanced logging and administrative capabilities of SafeQ, with the support provided MJ Flood, will enable data controllers and data processors to duly fulfill the relevant prevention and notification obligations under GDPR.

As part of a broader system of organisational and technical measures which every data controller and data processor must adopt, MJ Flood can confirm that with SafeQ under GDPR, customers will have the tools that enable the fulfillment of the personally identifiable data protection requirements for an individual's right to request and or delete personally identifiable information.

To satisfy an individual's right to request the personally identifiable data an organisation has within SafeQ, an authorised IT personnel member can use SafeQ's Reporting module to run a user report and filter results specific for the individual user. Additionally, the IT personnel member can use the SafeQ administrator's web management interface to display all attributes for the individual user. Data in other areas (such as personal data in logs or in user records of the Payment System, if any are present) can also be identified and filtered, should the need arise.

To satisfy an individual's right to be forgotten, once an IT administrator removes the individual from the company directory, the individual is automatically removed from SafeQ system. If the individual requesting the right to be forgotten still needs to remain in the corporate directory, the SafeQ administrator can make a manual deletion in SafeQ's administrator user interface.

To ensure compliance with GDPR Regulation for your print, scan, copy and fax systems, please contact MJ Flood on 01- 466 3500 or email james.kavanagh@mjflood.ie