

Lexmark apparaten zijn AVG-ready en bieden meerdere ingebouwde beveiligingsfuncties waarmee de klant over alle security-aspecten beschikt welke vanuit de AVG wetgeving aan dergelijke apparatuur wordt gesteld. De beveiligingsfuncties zijn beschikbaar over de gehele productlijn en omvatten toegangscontroles, controlelogboeken en ingesloten OS-beveiligingen. Diverse beveiligingsfuncties welke concurrenten nu pas integreren binnen hun apparatuur zijn binnen Lexmark apparatuur al jaren standaard.

- Versleutelde en ondertekende firmware zorgt ervoor dat alleen firmware die ontwikkeld is door Lexmark geïnstalleerd kan worden op Lexmark apparatuur.
- Veilige opstarttechnologie valideert of de firmware op de printers echt van Lexmark afkomstig is en informeert gebruikers als dat niet het geval is.
- Functies als toegangsbeveiliging beperken wie welke apparaat mag en kan gebruiken.
- Functies als netwerkbeveiliging beschermen apparaten tegen ongeoorloofde toegang via netwerkinterfaces.
- Functies als documentbeveiliging zorgen ervoor dat documenten niet in verkeerde handen vallen of ongeoorloofd zichtbaar zijn.
- Beveiligd remote beheer biedt een breed scala aan hulpmiddelen en apparaat mogelijkheden om effectief een groot aantal netwerk laserprinters en multifunctionals te beheren.
- Harde schijf beveiliging beschermd Lexmark printers en multifunctionals welke een interne harde schijf bezitten met een virtueel scherm.

