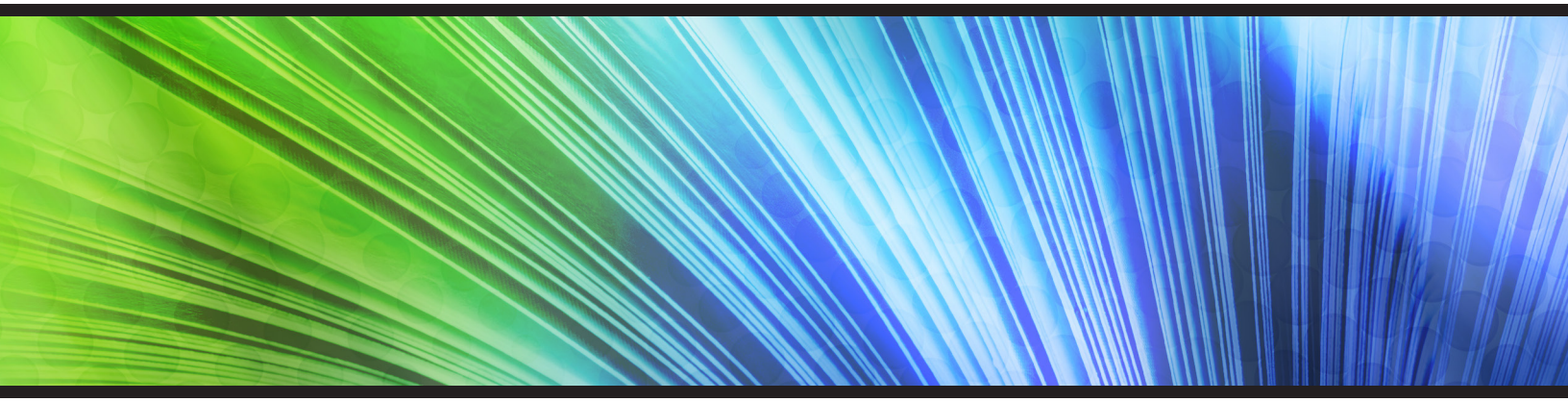

FAQ: GDPR and LRS® Output Management Software

Potential GDPR violations when printing and how LRS solutions address these.

What is the link between output management and GDPR?

The new General Data Protection Regulation (GDPR) regulation comes into effect on the 25th of May 2018. The goals of the regulation are to create a single data protection legal framework across the EU to provide individuals with control over their personal data, and to implement data protection/data privacy rules on companies that collect, store, and process such data.

Personal data is anything that allows a person (data subject) to be directly or indirectly identified. This data could include a name, an address, or an email address. It could be for an individual who is a customer, a partner or an employee. Ultimately, if it is personal data about a living person, companies are now liable to secure and manage that data in line with the impending regulations. Personal data in businesses is generally stored in two main ways; either electronically or in paper form. It is here that the GDPR and output management align.

Output Management software manages the capture and delivery of documents to a broad range of print devices and softcopy (electronic) destinations. These documents are generated by desktop, mobile, and enterprise applications (e.g., ERP, EMR, CRM, etc.), and they may contain personal information that must be safeguarded for GDPR compliance.

Can LRS software make us GDPR compliant?

No. On its own, LRS software cannot make an organization fully GDPR compliant because GDPR and its impact on your business goes beyond documents and their storage. Each business works differently, has different processes and manages their personal data differently – therefore there is not a single cookie-cutter approach to "getting" compliance. We can say however that LRS software can aid your organization in making its printing processes more GDPR compliant. One thing made clear in the GDPR documentation is that organizations will need to demonstrate that they have implemented the appropriate technology and operational safeguards that protects personal data.

Can you create a report to show who printed What, Where and When?

Yes, we can do this. Audit trails that prove who printed what documents are an important took for understanding a possible data leak.

For example: imagine a user prints a highly secure document with LRS pull printing, and later this document is identified to have been leaked. Administrators can search through the LRS audit reporting system and logs to show which employee/s have printed the document.

How LRS solutions successfully protect your sensitive data while printing.

Visit LRSOutputManagement.com/secure-printing to learn more.

How can LRS software support customer requirements in relation to the rights of the individual within GDPR?

LRS software provides secure printing for all output and print from any application to any device. LRS customers can:

- Protect print data “at the device” while it is printing (through what is commonly known as pull printing)
- Protect print data “in motion” on the network (encryption)
- Protect print data “at rest” on print servers
- Audit (track) all print activity
- Use watermarks, timestamps, and other security features
- Enforce copy and tamper protection when required

All of the aforementioned features strengthen privacy, control access and (in the event of a breach) enable an audit trail for printing of personal data. This comprehensive approach protects personal data from the moment it leaves an application, desktop or mobile device until it reaches its destination either in printed or electronic format.

Do LRS solutions store personal data within the software?

No, LRS software does not “store” personal data within its software. Documents are processed through the software and transmitted until they reach their destination either on a printer or electronically storage. The LRS auditing system does record the user and document names, but this information can be redacted if required.

Can LRS Software limit the rights for copying and printing certain documents?

With the LRS solution, organizations can control which users have rights (access) to specific MFP functions. This means that organizations can control printing, scanning, faxing and copying functions based on the job responsibilities of individuals/groups. For example, user “A” is allowed to print documents but not scan whilst user “B” can do both. The detailed level of rights management varies by printer manufacturer based on the design of their respective hardware platforms. LRS also supports several ways to authenticate at the printer and can be configured to require two layers of authentication (dual factor - card/badge plus PIN), if necessary, for added security.

Can LRS software add identifiers to documents as they are printed or stored?

LRS software can add on identifiers like user ID’s, dates, locations, barcodes or something similar which proves when and where a document originated from. This metadata can be embedded directly into the data stream sent to the printer or other output destination.

LEARN MORE

- Infographic
- Blog
- Case studies
- Checklist

How LRS solutions successfully protect your sensitive data while printing.

Visit LRSOutputManagement.com/secure-printing to learn more.

LRS® OUTPUT MANAGEMENT

www.LRSOutputManagement.com