

Whitepaper

GDPR: How dematerialization of paper documents can help you to understand the GDPR?



Alaris

a Kodak Alaris business

Summary

Introduction	3
1. The 7 principles of the GDPR	5
2. The best time to collect paper data	7
3. Dematerialization tools, essential elements for compliance	9
4. The processing register as evidence	14
5. The 7 concrete advantages of digital processes	15
Executive Summary	17
Alaris at the service of digital transformation	18



Introduction



The new EU Data Protection Regulation (GDPR*) entered into force on 1 May 2018. It ensures uniform rules on the protection of personal data.

In the months preceding the entry into force of the Regulation, data protection principles were sometimes treated in a secondary way, due to the lack of sanctions and a concrete framework. The rules are now established and the consequences for companies that do not comply with this privacy policy are known. Since May 2018, in the event of non-compliance, the supervisory authority has been able to apply several sanctions, including a fine of up to 4% of annual turnover.

If no personal data are concerned, the GDPR does not intervene.

However, the meaning of the term «personal data» is very broad. It includes, for example, information such as a person's name, address, telephone number, license plate number, but also their IP address. It is sufficient that the information is simply assigned to a person so that the person can be identified. Thus, each company will have to comply with the implementation of the GDPR, failure to comply with this regulation being subject to severe penalties.

The GDPR covers not only digital data but also paper data.

One of the complexities of this subject concerns the type of media involved. If the notion of digital data comes to mind immediately, it is important to note that paper documents are also affected by the GDPR. And it is a much more difficult part to map: application documents, order forms, loan applications, contracts, business cards or even simple notepads are just some of the many examples of documents containing personal data.

In addition, many processes are sometimes carried out exclusively on paper, depending on the level of digital transformation of the structure and its sensitivity to digital. For example, employee data, time sheets, invoices or customer contracts are not spared by the GDPR.

For several years now, more and more companies have been engaging in dematerialization phases and transferring their data to servers or cloud services. This is for two reasons:

- File storage takes up a lot of space and represents a certain long-term cost
- Data structuring

*GDPR: European Data Protection Regulation



Prerequisites for setting up a data structuring system

The DGMP requires the processing of both digital and paper data.

It is therefore essential to ask the right questions:

- Which documents contain personal data?
- Who has access to these documents?
- How to find these documents?

It quickly becomes clear that it is difficult to answer these questions in practice through paper processes. A storage system, however detailed and clear it may be, struggles to meet the new data security guidelines.

The following four questions highlight risks for which dematerialization can be an effective solution.

Which documents contain personal data?

A curriculum vitae, a certificate of illness or a request for leave, etc. Personal data: personal data are found in the company's official documents, which are subject to specific protection. Companies need to know which documents contain sensitive data and consider them confidential. Thus, for companies where customer relations are at the heart of their activities, we think, for example, of loan requests or documents relating to health: the panel is large.

Who has access to these documents?

It is difficult to protect confidential information when it is on paper and most companies are not always able to control access to it. Indeed, it may be possible for several people in the company to consult these data. These physical accesses then become even more difficult to identify.

How to find these documents?

On the basis of the «right to forget» (Art. 17 GDPR), it is possible for the customer to request the deletion of his data. This can only be done if companies know where personal data is stored. Paper documents are generally archived by date of receipt or type of document, not by content.

In addition to these constraints, Article 20 of the

Another example of a complex rule to be implemented is the GDPR «right to data portability»: a person has the right to take his or her personal data with him or her when changing suppliers.

If necessary, a company must therefore make all customer data available in a structured, common and readable format.

So what kind of tools should be used?

The solution is to migrate to digital processes to facilitate the implementation of the GDPR. Otherwise, it would be more complex to comply with the strict rules of data protection. Those who scan paper documents can better protect, manage and control information.

Digitization is therefore the first step towards compliance. It requires the choice of the scanner and more precisely an intelligent scanner, since it can be coupled with a capture software that will feed the monitoring and proper functioning of the GED, also known as electronic document management. Capture tools will allow you to read and process your data in intelligent and secure ways to index and classify them within your organization.

1. The 7 principles of the GDPR

The GDPR can be summarized into 7 key principles. These 7 principles have different relevance for the digitization and data collection process:

- 1 ▪ **Legality, traceability, voluntary consent, transparency**
- 2 ▪ **Purpose limitation**
- 3 ▪ **Data minimization**
- 4 ▪ **Accuracy**
- 5 ▪ **Storage limitation**
- 6 ▪ **Integrity and confidentiality**
- 7 ▪ **Responsibility / accountability**

Principle 1 - Legality, traceability, voluntary consent, transparency

The exchange with an individual wishing to have information about his data must be understandable, unambiguous and in accordance with the principles of good faith.

Behind this principle lies the right to information, access to information and self-determination (The term self-determination means that your interlocutor has the right to decide for himself what you can do with his data).

It is therefore necessary to use tools thinking in terms of

«data protection». This means that even when planning a project

(e.g., mailroom creation or redesign), processes and choice of hardware and software (hardware/software) must comply with the DGMP guidelines. In addition, data protection must already be defined in the standard

«By default», and can only be enabled or disabled at the operator's initiative.

Principle 2 - Purpose limitation

It describes the assignment of data. They may only be used for specified, explicit and legitimate purposes. For example, if you collect an email to send a document, you cannot use this email address for anything else, such as a sales campaign. You may therefore only process the data for the purpose for which you have collected them.



Principle 3 - Data Minimization

It refers to the minimization of data in order to keep only an appropriate quantity for the purpose for which they are intended.

In short, it is a question of limiting the quantity to what is strictly necessary.

Principle 4 - Accuracy

It focuses on data matching. These must be accurate and up to date, while erroneous data must be erased or corrected.

Principle 5 - Storage limitation

It describes the limitation of data accumulation. These can only be kept and stored to the necessary extent.

Principle 6 - Integrity and confidentiality

It guarantees the integrity and confidentiality of the data. It is mainly about protection against unauthorized processing, loss, destruction or damage of data. The GDPR explicitly requires «appropriate technical and organisational measures» to avoid such cases.

Principle 7 - Responsibility / Accountability

It addresses responsibility/accountability as well as documentation requirements, i.e. to provide evidence of compliance with the DGMP. The security measures (described above) are directly integrated into the description of procedures.



2. The best time for the collection of paper data

«We have established that compliance is more affordable through a dematerialization process. However, before introducing any notion of dematerialization, it is necessary to go through the digitization phase, i.e. at the time of the conversion of the physical medium into digital data.

«The procedures for collecting paper data can be defined in three classes:

Early centralized capture

Paper documents, grouped in a central mailroom (Digital Mailroom), are scanned centrally. It requires a series of essential but costly manual actions: the preparation of documents or their post-processing, and sometimes manual indexing.

Early collection means that documents are digitized before any further processing by the company. This procedure ensures paperless operation in the following processes.

Late centralized capture

Late capture means that paper documents are first physically present in the company and are part of the internal transaction processing. Only after the end of the operation are the documents digitized in a central scanning unit. This is a pure archiving operation.



Decentralized capture based on transactions

Decentralized recording eliminates the spatial and temporal disadvantage of physical paper transport. Documents are scanned as soon as they are available.

The employee in charge of the current business operation scans the documents and assigns them the corresponding key information. This approach is also called «transaction-based collection».

The fact that the information, instantly digitised, is immediately available for further processing is a significant advantage. In addition, this approach makes it possible to integrate not only internal departments and subsidiaries, but also customers, suppliers, agencies or external employees. These procedures, which now complement the central mailroom, will play a major role in the future, particularly for companies operating worldwide or companies with many branches.

So far, centralized capture has been sufficient in most cases. But in times of instant communication, increased mobility and high customer demands, decentralized digitization is a highly recommended solution. Scanning technologies and solutions allow paper documents to be linked to electronic processes in a simple, efficient and secure way.

In decentralized capture, it is absolutely necessary to note that scanners not only provide comfort, but also meet safety requirements, in the workplace or in various departments.



These procedures will play a major role in the future, especially for companies operating worldwide, or for companies with many branches.



3. Dematerialization tools, essential elements for compliance

Since the objective is to store the data, structure it and protect it to meet new compliance requirements, the choice of dematerialization tools will play a key role. We will focus here on the use of scanners and capture software and see how their functionalities reflect the new regulations. With the dematerialization process now underway, it is strongly recommended to continue on this path by acquiring a document management solution (DMS) to help you organize and manage your electronic data.

The importance of ensuring that your document management (DMS) solutions are properly powered by the acquisition of capture software

As a reminder, GED solutions will help you manage and organize your company's electronic data and information. Different systems are at your disposal: digitisation, indexing, archiving or even distribution, accessible in a single and highly secure platform.

Indeed, document management systems allow you to check what information has been accessed, by whom, and when.

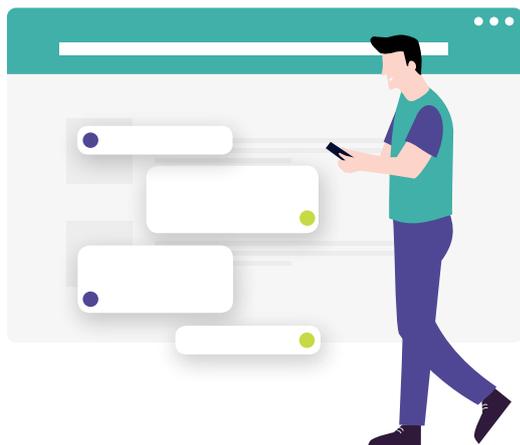
There are also ways to set up access rights to documents.

This way, you can exploit and control your data flows while maintaining traceability and action history. In the era of the DGMP, the efficiency in data control and traceability meets the compliance and security requirements of the new regulations.

It makes it all the more easy to provide proof of this. Not only are GED solutions a tool to promote compliance with the DGMP, they also avoid errors, time spent searching for information and losses. Therefore, they considerably increase your productivity and reduce the costs of manual management..



«The choice of an intelligent capture solution is crucial to the proper functioning of your DMS solutions. These software programs will recognize and extract information from documents, forward it and classify it in the systems where it should appear. It could be a local folder, a cloud location, an integrated range of business applications or an ECM.



How to choose your capture software?

This list identifies the fundamental qualities of capture software to meet the requirements for compliance with the GDPR.

The automation

Automation is the key to good capture software, the more it recognizes, learns and memorizes through artificial intelligence, the more time you will save and avoid errors.

Simplification

Simplifying and accessing information through easy-to-use capture software saves time and avoids waste.

The mobility

The capture software's ability to take mobility into account must be able to cover several workstations, but also several sites in your company. It can send data to local folders, the cloud or integrated applications.

Authentication

A digital data must be reliable and identifiable (for example, if it is derived from a paper document and the document is to be destroyed, as required by Article 4 of the GDPR), it is therefore essential that the capture software can meet this need.

Safety and security

Security must be a requirement for capture software. It must be able to help regulate access to data but also be able to closely monitor places where particularly sensitive and confidential information is held.

Respect for a 0% paper chain

As electronic document flows increase, you should choose your capture solution from the multi-source capture possibilities offered by the software.

Such a tool, capable of implementing the capture of e-mails as well as the capture of paper documents via a scanner, will be a major asset to accompany a transition to 0% paper.

Choosing the right scanner is the first step in the dematerialization process

The choice of an intelligent scanner

The choice of scanner, and more particularly a so-called «intelligent» scanner, is very important and remains rather unknown on the functionalities that simplify the dematerialization process. Beyond the aspect of speed and data backup, a scanner coupled with the right capture software can extract and index data, including optical character recognition (OCR). Using these tools, we obtain a file that allows us to filter data quickly and easily. Thus they can be deleted with a simple click, while documenting this deletion process.

When selecting a scanner, pay attention to the «intelligent document protection» setting. Thanks to ultrasonic technology, it detects an incorrect sheet feed and immediately interrupts the paper feed, in order to protect and avoid damage to the base document. In addition, an active sheet printing technology, known as

The active feed technology, used by high-volume scanners, helps to avoid false and multiple prints.

Good image quality can be guaranteed - even without the use of powerful PCs - so that it is suitable for use by customers using the web environment. Data extraction can also be optimized by intelligently reading barcodes that provide the most accurate information possible.

«It is also important that you know how to scan documents correctly, but also be aware of the functionalities of capture software, in order to meet the requirements of the GDPR with complete peace of mind. Indeed, even for the scanner and the capture software regulations exist. In order to help you in your efforts, we have developed a checklist:

- Scanner - GDPR
- Capture software - GDPR

This list contains the functionalities of a scanner or capture software by making a direct or indirect link with the GDPR.

You can use it to check your current or planned installations, and thus minimize your risks.

We used a concrete example to illustrate our point: the Alaris S2000 scanners and the Alaris Info Input Solution software. However, the table also applies to other manufacturers and other types of scanners or other compact capture software.



**When selecting a scanner,
pay attention to the
« intelligent document
protection » setting.**



Features and functions Alaris S2000 Series Scanner

Requirement, GDPR principle

Duplicate detection

Principles 1, 2, 3, 3, 5 and 6
Traceability, accessibility, data limitation, reduction in storage and data purpose.

Visual and interactive detection of the double power supply

Principle 6
Protection against loss, destruction or damage of data

Deleting blank pages based on content

Principle 6
Protection against loss, destruction or damage of data

Controlled document output

Principles 1, 2, 3, 3, 5 and 6
Traceability, accessibility, limitation of the data, decrease in storage and the purpose of the data

Fully automatic profile selection

Principles 1, 2 and 6
Traceability, purpose limitation and data integrity

Barcode reading

Principles 2, 4 and 6
Protection, purpose limitation and accuracy of the data

Integrated image processing

Principles 4 and 6
Protection, readability and accuracy of the data

Automatic alignment and cutting

Principle 6
Protection against loss, destruction or damage of data

Removal of bent edges, holes perforated, edges and scratches

Principle 6
Protection against loss, destruction or damage of data



Capture software (Alaris Info Input Solution)

Requirement, GDPR principle

Complete optical control of all images for high-speed scanning

Principles 4 and 6

Protection against loss, destruction or damage of data.
Accuracy of the data.

Protection against accidental movement, deletion, replacement and attachment etc.

Principles 4 and 6

Protection against loss, destruction or damage of data.
Accuracy of the data.

Selective authorization and access concepts (group and user permissions) for complete work and activation/lockout of individual functions

Principles 1, 2, 4, 6 and 7

Accuracy, traceability, limitation of the purpose and integrity of the data.
Proof of conformity.

Techniques for encrypting images and metadata during data transmission

Principles 1, 2, 4, 6 and 7

Protection against loss, destruction or damage of data. Accuracy, limitation of the purpose and traceability of the data. Proof of conformity.

Qualified digital electronic signature and digital fingerprint

Principles 2, 6 and 7

Protection against loss, destruction or damage of data and limitation of the purpose of the data.
Proof of conformity.

Secure document separation by barcode, patch, OCR, manual etc.

Principles 1, 2, 3, 3, 4, 5, 6 and 7

Protection against loss, destruction or damage of data. Limitation of data and purpose. Accuracy and traceability of the data.
Proof of conformity.

Deleting blank pages based on content

Principle 6

Protection against loss, destruction or damage of data

Fully automatic profile selection

Principles 1, 2 and 6

Traceability, limitation of the purpose and integrity of the data

4. The processing register as evidence

Keeping a record of processing activities is mandatory for all structures,

regardless of their size, as provided for in Article 30 of the GDPR. However, for those with less than 250 employees, a derogation exists for occasional/non-recurrent processing.

For this reason, we recommend that you develop a list of data mining activities.

This will give you an overview of the processing procedures, software and cloud solutions in your own company. And, in the case of a general inspection where you will have to prove compliance with the GDPR (Art. 5, §2), this can be done quickly.

What should be found in a processing logbook?

- The stakeholders (representatives, subcontractors, co-responsible persons, etc.) who are involved in the processing of the data,
- The categories of data processed,
- The purpose of the data (what you do with it), who accesses the data and to whom it is disclosed,
- The storage time,
- The process of securing data (especially with the existence of a reliable copy).

As part of paper processes, the creation and updating of such a directory requires immense efforts, depending on the size of the company. Dedicated software to trace or reconstruct processes facilitates the process and the integration of paper documents into the chain.



5. The 7 concrete advantages of digital processes

In addition to the obligation to comply with the new data protection regulations, there are other elements in favour of the digitisation of processes. Due to the significant but necessary manual effort, the expensive processing of paper is time-consuming in all sectors of activity. In an era where communication is almost instantaneous and mobility is a must, paper-based processes are no longer viable. You too can benefit from the decisive advantages of dematerialization.

1. The organization

You avoid the risk of sorting documents or archiving them incorrectly. Once digitized, documents are simpler to find, accessible and easy to transmit. The valuable time saved can be used for other business priorities, such as customer service.

2. Efficiency and effectiveness

Digitized documents are much easier to manage, store and access than paper versions. The ability to view them at any time and share them with customers improves team productivity and the customer experience. Automatic extraction of data from a scanned file takes much less time and is much less prone to errors than manual copying of data.

3. Scalability

The amount of data a company receives daily is constantly increasing. With the digitization of data, these quantities can be managed more easily. In addition, the personnel costs required to process large quantities of orders - at peak times or in the event of rapid expansion - are much lower.





You will know if your company is one of the winners or losers of digital transformation.



4. Respect for the environment

Less paper consumption means fewer trees used for production. In addition, paper generates high energy consumption, both in production and in transport. On the way to paper abandonment, the environmental aspect is therefore a good argument to have the support of the people involved in these issues.

5. Faster communication

Paper documents need at least one day to arrive from point A to point B. In addition, there are unforeseeable circumstances such as delays, incorrect deliveries or even the total loss of paper. On the other hand, scanning allows immediate access to a document.

6. Backup and recovery

It is expensive, time-consuming and even impossible to replace a paper document in the event of damage or loss. In addition, disasters such as fire or floods can lead to significant loss of information. In a dematerialized office, documents are transmitted to a server or cloud service that provides an easy, fast and secure electronic backup of your important information.

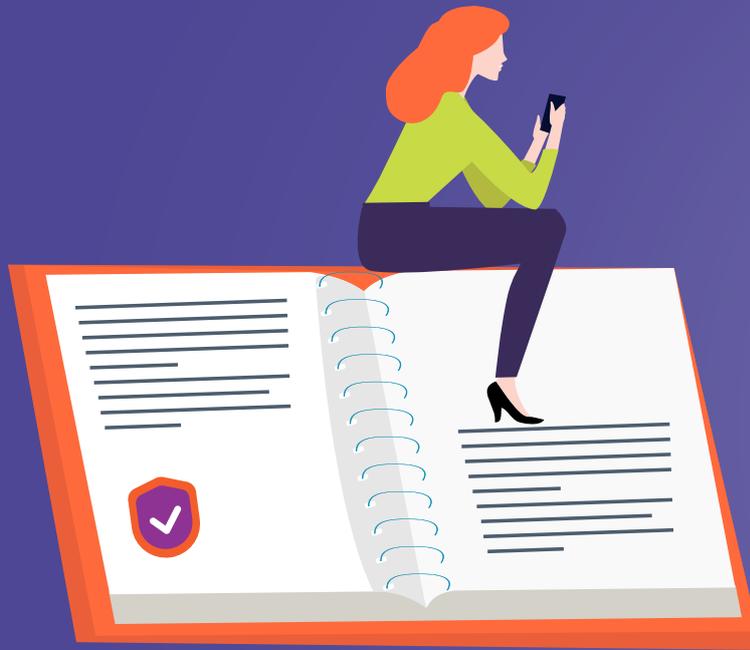
7. The profitability

Companies can avoid storage and printing costs by switching to digital documents. The increase or release of storage space can be used in other ways.

Digital transformation affects all sectors of activity as well as companies of all sizes. In the future, it will even determine the competitiveness of a company.

In the next five to ten years, you will know if your company is one of the winners or losers of digital transformation.





Executive Summary

As we have seen throughout this white paper, the GDPR contains requirements that can be met through digital processes. How can we guarantee, by continuing to work mainly with paper documents, that all of a person's data can be retrieved or even deleted? In addition, the accuracy of paper data is not always evident. Finally, how can it be ensured that personal data are kept as long as required by the regulations when they are dispersed in different filing cabinets, dusty and exposed to various types of damage?

The GDPR as a driver of digital transformation

It is no coincidence that the general data protection regulation contains such strict requirements. The Regulation applies to the current state of the art and requires that the benefits of the technology be made available to data protection. In this way, it advances the familiar subject of digital transformation. This is another reason to take up the challenge of the digitisation process and to take advantage of a number of the benefits it generates.

In addition to the fact that the right intelligent lead or customer relationship management (CRM) systems make it easier to take the DGMP into account, digital transformation still promises considerable advantages. As a result, companies benefit from legal certainty, automation and flexibility, with increased efficiency.

Alaris at the service of digital transformation

Alaris, a division of Kodak Alaris, is an expert in information capture solutions that simplify business processes. We help to make sense of information with intelligent and connected solutions that are the result of decades of innovation.

Our range of award-winning scanners, software and services meets the requirements of both companies and administrations in their digital transformation and dematerialization projects.

You want to know more about Alaris?

Visit Alaris the Mag:
blog.alarisworld.com
or the website
www.alarisworld.com

