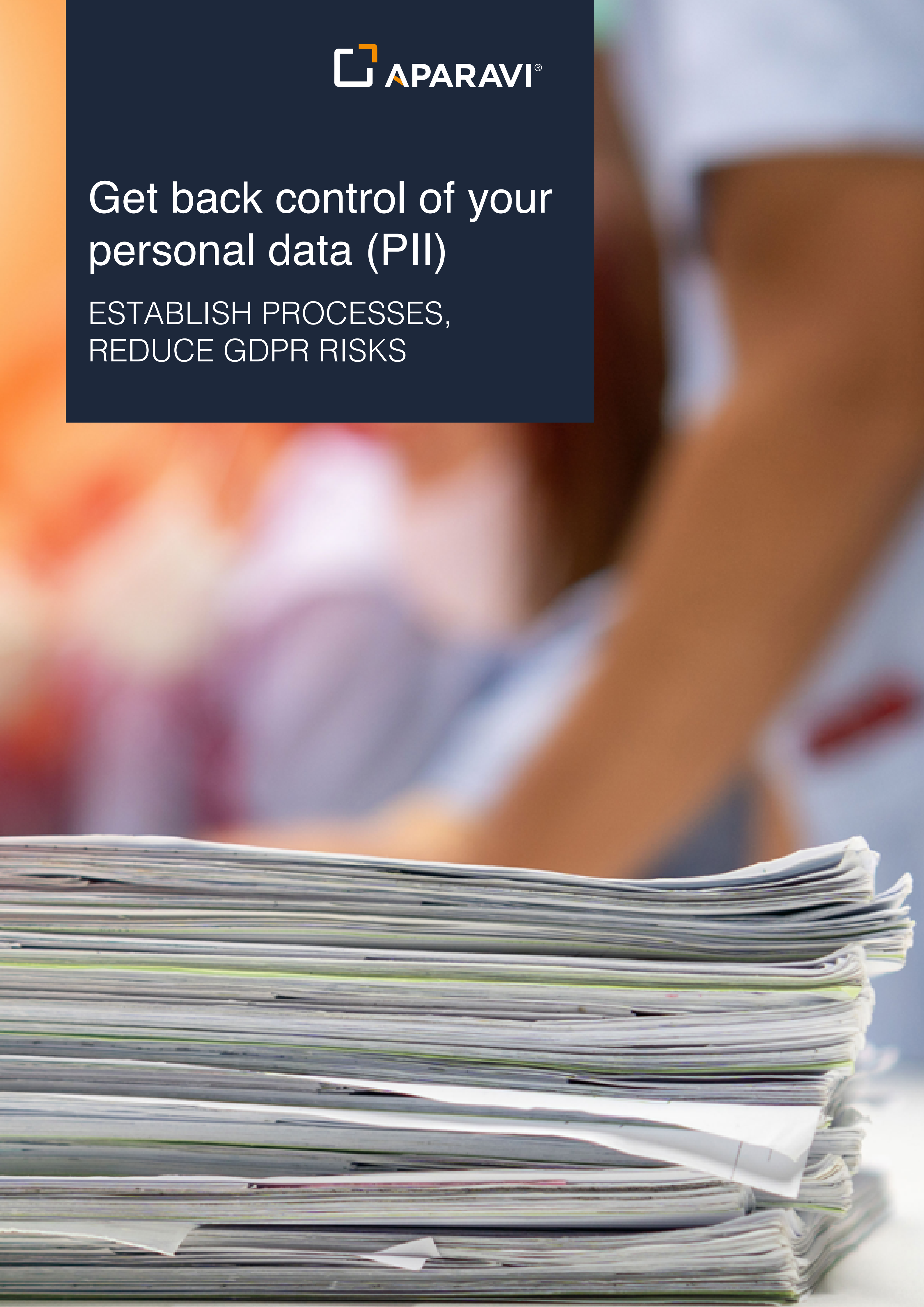
APARAVI®

Get back control of your personal data (PII)

ESTABLISH PROCESSES, REDUCE GDPR RISKS



Get back control of your personal data (PII)

Lack of transparency and control

Do you have full transparency and control over all your personal data?

No? Don’t worry, hardly any company is able to answer this question with “Yes!”. Did you know that only 20% of a company’s data is structured? 80% of the data is unstructured – often unused, unusable, or unknown. That presents companies with a big challenge, especially in terms of GDPR.

Lack of intelligence and close to zero automation

According to GDPR rules, personal data from customers, employees, applicants or suppliers may only be stored in determined systems with restricted access rights and appropriate security measures. Nevertheless, this sensitive data is often widely distributed in the internal storage. Sometimes there are even multiple copies of one file, that is unknowingly included in unstructured data. Companies are not able to handle the resulting GDPR risks without a suitable automation strategy.

Professionalising data protection

The protection of personal data is no coincidence, it’s a result of a long term, sophisticated strategy. The development of deletion concepts, the fulfilment of accountability, a clear approach towards a fast response to GDPR inquiries from customers and a proper documentation are required to work target oriented.

This whitepaper shows you, how to overcome operational obstacles in holding and analysing unstructured data, with a special focus on the automation of requests for information and deletion according to article 15 and 17 GDPR. Get back full control over your personal data!

Get back control of your personal data (PII)

Lack of transparency and control

The challenge: Data protection often fails for operational reasons

No company ever says:“Today, we’d like to violate the GDPR.” Just the opposite. Most companies and authorities make a big effort to safeguard the sensitive data their customers or citizens have entrusted to them. And that is indeed revealing: They are always “making an effort”. Companies are still too often failing to actuallyclear the operational hurdles involved in complying with the provisions of the General Data Protection Regulation (GDPR) – especially when it comes to taking stock of and analyzing unstructured data.

GDPR violations are expensive and harmful to the business

It happens to the best: H&M, British Airways and TIM, the biggest telecommunication company in Italy, are only a few examples. All companies had to pay high fines due to GDPR violations. Additionally, the number of former and current employees who report their employer for data protection violations is drastically increasing.

- **Personal liability of management,** until valid proof can be provided regarding-the origin of the damage
- **Loss of reputation and trust**, which can lead to problems with supply chains, capital procurement and lost can lead to fall of revenue
- **Cost for eliminating** the cause of the data breach
- **Intangible claims for damages up to 50,000 euros**
- **Purchasing and introducing tools Tools** and processes for maintaining GDPR compliant structures and data pools in the future
- **Higher expenses for recertification, e.g. ISO, TISAX** due to insufficient technical-organizational measures and negligent data leakage
- **Fines,** that can be as high as 20 million euros or 4% of annual worldwide turnover

Get back control of your personal data (PII)

Know your data: Manage securely information & deletion requests

Requests for information and deletion: Error-prone and time-consuming processes

GDPR compliant data management does not only include the storage and management of data, but also the complete processing of information and deletion requests on time. Companies are obligated to implement an adequate infrastructure to meet these requirements.

Growing challenge: Large unknown dangers lurk in unstructured data

As previously mentioned, hardly any company can provide complete and accurate information about personal data, not to mention the execution of a comprehensive and legally compliant deletion. The complete transparency and control over these sensitive information in unstructured data like Office files, PDFs, CRM/ERP exports and pictures is lacking.

Classify and inventory your unstructured data fast and comprehensive. And implement a professional data management on a secure basis!

But which regulatory requirements does the GDPR impose with regard to personal data? Here are the key articles:

- **Art. 12**: Fulfilling the duty to inform the data subject transparently
- **Art. 15 to 21:** Responding to requests- from the data subject
- **Art. 5, 17:** Defining a data deletion policy
- **Art. 33, 34:** Duty to notify authorities and data subjects of a data breach

Get back control of your personal data (PII)

Know your data: Manage securely information & deletion requests

Requests for information and deletion also concern unstructured data!

You probably already have a suitable software to search your structured data base and can easily retrieve sensitive data from CRM & ERP-systems. But how can you make sure that all personal data in your unstructured data base is found?

Fast growing number of requests for information and deletion

Technologically, due to digitalization and automation the fast and error-free processing has long been possible. But reality is different: A request via email, letter or fax arrives at the company, a customer or former employee requests information and/or deletion of his/her personal data. Do you even know what data you are processing, where the data is stored and based on which legal basis this data is processed?

The hard reality: Manual, time-consuming and error-prone processes all-over

Presumably one or two employees are spending a lot of time to search for the information of the concerned person in the common CRM, ERP, and HR softwares. However, this is not where all personal data resides. Data that is internally transmitted from one department to another like CVs, locally saved pictures from IDs, Excel files with personal data and many more, is often forgotten.

The consequences of manually processing the request for information and deletion and the GDPR compliant inventory of the company's data, are overworked employees and wasted working time to find the data and error-prone processes!

Get back control of your personal data (PII)

Significantly reduce risks in a structured way

Establish an efficient and permanent data protection management in 4 steps with APARAVI

1. Request for information or deletion

An email with a request for information or deletion was sent to e.g. privacy@yourcompany.de, personal data is read out and the APARAVI scan starts with your database – no matter if on premises or in the cloud. Written requests via fax or letter are processed customer-specific: Scanned documents can be included in the digital process or handed over to the authorised employee. Or the data is quickly and easily entered into individual search interfaces to start the process.

2. Identification of affected data

The query results are shown after a few minutes in any list. Sharepoint lists are best suited, as specific actions like “download”, “delete”, “share” can be directly integrated. The affected files are quickly, traceably, and clearly identifiable because file names, storage location, access rights, modification dates and meta- & content data as well as search context can be output.

3. Complete, error-free information

The responsible employees are now able to easily and securely verify the content of the files and move them to other specific designated storage locations. The query results can also be imported into existing systems, aggregated, edited (e.g. blackening) or directly sent to the affected person. Data from structured and unstructured sources result in a detailed, legally compliant and court proof request for information.

4. Simple, reliable deletion

More than half of the information requests result in a subsequent request for deletion. Similar to an information request, the deletion also requires extensive research to obtain a complete overview of all known and unknown storage locations of the personal data. Standardised or self-defined deletion concepts should be used, to ensure legally compliant data deletion on time.

Get back control of your personal data (PII)

Significantly reduce risks in a structured way

Your APARAVI advantages at a glance

Simple, fast and error-free provision of information

– Reliable detection of sensitive data in unstructured, unknown data estates

– Complete and legally compliant deletion of personal data

– Integrable in every system via API: Aggregated information from structured and unstructured data

100% control and legal security

– Compliance with GDPR criteria: Part of the granting of DIN27001/TISAX certification through technical and organisational measures

– Clean & lean data base: Classified and inventoried data base

– Create legally compliant reports for audits automatically

Everything at a glance and one click!

– Reporting Dashboard: Analysis of over 6,000 file types with adjustable classifications to identify and resolve data risks

– Standardised and individual scans: Queries and classifications to meet specific requirements for personal data

Professional risk based measures

– Detect security risks at an early stage through regularly taking inventory of your files and unstructured data base for e.g. SMB fileservers, OneDrive, Sharepoint, Azure Blob, AWS S3 and many more

– Privacy Impact Assessment: Derive risk-based measures through continuous risk evaluation

Get back control of your personal data (PII)

There is a clear winner:
Prevention vs. intervention

Approach data protection proactively!

You always want to be one step ahead when it comes to data protection? Perfect, because APARAVI supports perfectly in preventive, continuous use. Invest sensibly and in a long-term planned manner in technical-organizational measures! Because follow-up costs are much more than just fines! GDPR violations quickly cost you a lot of money: high fines, claims for damages, the cleanup of data outflows and loss of reputation.

With the permanent use of APARAVI, you avoid expensive, labor-intensive and undocumented individual measures and thus create an important building block for an established, professional data protection management.

Rely on APARAVI:

- **Minimize risk of GDPR violations** occurring in a lasting, sustainable manner
- **Avoid unnecessary costs resulting** from the damage to your reputation,claims for compensation and loss of certificates which follow data violations
- **Eliminate the risk of personal liability** for your executive management
- **Legal certainty and peaceful nights** for your data protection officers and information security officers
- **Active communication** of highly professional data protection management increases customer loyalty

Get back control of your personal data (PII)

Contact us!

Smart and safe!

You want to reduce your GDPR risks significantly and answer requests for information and deletion fast and correct?
We show you, how to perfectly get a grip on your management of unstructured data in just a few weeks.

Talk to our GDPR experts and test APARAVI for free!

Telephon: +49 (0)89 7406 2578
E-Mail: sales.eu@aparavi.com

www.aparavi.com

APARAVI Software Europe GmbH
Lothstrasse 5
80335 München