GENERAL DATA PROTECTION REGULATION (GDPR)

Turning a Challenge into an Opportunity

The GDPR landscape

As of May 2018, non-compliance with GDPR (General Data Protection Regulation) can be punished with severe penalties of up to 4 % of total turnover or 20 MEURO, as well as the cost of compensation claims. GDPR applies to any organization located in the EU (European Union) dealing with information related to individuals. It also affects companies from outside the EU that promote their services within the EU and process personal data of individuals ("data subjects"). This means that GDPR is high on the agenda for many large organizations, both within and outside the EU. Most affected are B2C segments like Banking, Insurance, Healthcare, Telecoms, Legal and Education, etc.

In principle the approach to GDPR compliance is simple; companies assess how GDPR impacts their business, gaps are identified and measures are taken. In practice it's more complex; assessments typically show that only a small portion of companies are compliant and don't have full visibility of where and how in-scope information is held This creates a high level of risk, as not knowing that information exists will not be accepted as an excuse. The burning issues are:

- Policies, controls, processes, roles and responsibilities in handling personal data
- Acquisition, storage, retrieval, processing, usage, change and destruction of personal data
- Manageability of digital and physical data in a structured or un-structured format
- Confidentiality, integrity, security, availability and resilience of data handling
- IT platforms, systems, databases
- Transparency rules, information obligations and audit rights

The fundamental issues

At first sight GDPR is a regulatory topic, but the real issue is more fundamental: the structure of data, processes and communication. Often these structures have grown over decades, resulting in a variety of physical and digital formats (paper, tape, mail, records, …), containing structured and un-structured information (letters, mails, conversations, forms) as well as a broad range of storage locations (physical archives, distributed databases).

Despite all the publicity about GDPR not much has been said about paper records, when in reality, it's the area most likely to cause operational problems and expose organizations to risk. Paper is a real problem for GDPR. It can be held just about anywhere and any sheet of paper could contain personal data. It's also a problem of scale: as well as in-house filing, storage companies are holding 10's of millions of boxes and files. Much of this information has no meta-data and may be beyond the required retention period, but it will almost certainly contain personal data and as such it's a risk.

GDPR projects are underway, involving a broad range of business functions and staff. The volume and distribution of paper records means that it will take considerable time and effort to comply. The costs of these initiatives are significant with limited business benefit. Solutions are required that keep these costs to a minimum and also encompass the use of personal data for innovating and improving document and information processes. Taking a strategic view will allow businesses to turn a regulatory burden into a business enabler. GDPR is an opportunity to leverage the existing pool of data by making it actionable and manageable.

Solve the fundamental issue at the core of GDPR

Typical GDPR programs include these steps:

1. Creation of awareness and C–level support
2. Identification of processes and media containing personal data
3. Assessment of current processes, contracts and data objects related to personal data
4. Identification of gaps vs. GDPR requirements

5. Impact and risk analysis
6. Definition, funding and implementation of measures and projects

The outcomes of these programs are revised corporate guidelines, controls, reporting and auditing structures, as well as significant ICT-changes in the domain of databases, archiving, content management, CRM and ERP, access rights and identity management. The main issue is gaining control over a growing pool of physical and electronic documents, in structured and unstructured form, as a pre-condition of GDPR compliance. This involves:

- Finding and identifying personal data
- Tagging, indexing and classifying available personal data
- Gaining explicit consent from data subjects on personal data and its purpose
- Communicating, modifying and deleting personal data on request
- Gathering, documenting and enforcing usage limitations and permissions

Few businesses are paper-free. Some have islands of digitization or some paper free processes but wholesale change to a digital model has been much slower than the industry pundits suggest. GDPR initiatives that don't involve digitization will drive up process costs and won't deliver increased agility. As a result, customer experience, innovation and competitiveness are obstructed. Going digital at the doorway doesn't just make GDPR compliance easier it creates value across the business. The most successful GDPR programs go beyond formal compliance and regulation by reconsidering the overall approach to document and information processing and opening the door to a much wider range of benefits. This requires a forward looking approach.

Addressing the root causes and creating business benefit

Data is a strategic asset. The availability of actionable data creates valuable new business opportunities, entire new worlds of customer experience, new levels of operational excellence and drives obsolescence of legacy systems and processes. Digital delivery dramatically reduces mail handling, document management costs and information processing times. But many struggle with this due to un-structured data and the variety of electronic and physical media used; the same obstacles companies face in their GDPR initiatives. Therefore, it would be short-sighted to tackle this topic from a purely GDPR perspective.

The cost and challenges faced when implementing GDPR programs are a direct result of a data legacy that has evolved over many years. This legacy is turning into a burden as processing of data becomes increasingly complex, both in general and for compliance purposes. The key questions are: shall we invest in turning a non-compliant legacy into a compliant legacy? or shall we invest into transforming this legacy into an asset for our future business? Should we accept the increasing cost of complexity of a legacy environment? or invest in a step-change to create new business opportunities? The tipping-point for this step-change has already arrived. Not addressing this fundamental issue has become a serious threat. Digitizing document and information processing creates an opportunity to:

- Improve productivity: access information at any time from any location and collaborate more effectively
- Improve customer satisfaction: back office services are aligned to customer demand for fast and well informed responses
- Improve customer insight: information contained in every communication is visible, creating a 3600 customer view, providing input for data analytics and informed decision making
- Improve compliance: full visibility and control enables a faster response to legislative changes, reducing risk and protecting reputations

Most companies have no policy on filing and no view of the legal status of the information contained in archived documents. The most onerous task will be digitizing legacy paper. In the headlong rush to meet the GDPR deadline some organizations may be tempted to destroy rather than digitize. Side-stepping regulations by destroying records is a very risky option, not to mention a waste of information capital. Done in the right way digitization will be a milestone towards becoming a fully digital enterprise; one that brings valuable information back into circulation.
GDPR is a wake-up call to prevent organizations from becoming digital laggards. The limiting factor for many companies is neither strategy, nor will, nor opportunity. It's often lack of resources, expertise and operational inheritance. Businesses can resolve this dilemma by selecting the right strategic partners. Outsourcing provides a pathway that addresses the fundamental issues of GDPR and harnesses digitization to ensure compliance, enable prompt handling of subject access requests and exploit new business opportunities.

SPS can help

SPS manages all personal data entering an organization, independent of form (physical, electronic) or format (structured/unstructured) using future-proof and compliant solutions and services. With a combination of highly efficient on and off-site service centers, scanning and recognition technology as well as artificial intelligence digital documents are created, relevant data is extracted and documents are accurately classified and indexed. Documents and information are processed efficiently, compliantly and to the highest quality standards as they enter the business. Physical documents are made uniquely identifiable and filed or destroyed in line with policies.

SPS moves processes relating to personal data into the digital world. Physical records only need to be touched at the beginning and the end of their lifecycle (single-touch-processing). In-between, all handling of information is digitized. The enabler for this approach is a (digital) mailroom combined with the intelligent processing of transactional data and documents. By digitizing existing physical archives, legacy data-pools are cleaned up and the operational burden of handling physical documents (retrieving, collection, tracking, etc.) is eliminated.

Based on a leading business processes services platform SPS creates new opportunities for the processing of personal data. Documents and information become action-

able from the very beginning of a process, so entire steps can be eliminated, automated or delivered from off-site service-centers. As a result, SPS services not only ensure GDPR compliance but also create additional benefits by deploying AI (Artificial Intelligence), RPA (Robotic Process Automation) and enabling data analytics, providing:

- GDPR compliant handling of legacy and newly acquired data
- Improving quality and speed of physical and digital document and information processes
- Cost reduction, operational agility and adaptive capacity
- Committed SLA and audit track
- Disaster recovery, back-up and crisis response capacity
- Enabling advanced business analytics by creating actionable data
- Continuous improvement and commitment to innovation

SPS services comply with GDPR by design and enabling customers to seize the opportunities of digital transformation. Experts in end-to-end data processing, from omni-channel input, through digitizing and processing, to omni-channel output, and with a strong track record in innovation, SPS is the ideal strategic partner, backed by the long-standing tradition of Swiss privacy and security. SPS customers get the best of two worlds: service excellence and innovation, paired with quality, security and trust in the areas of:

- Omni-channel Input Processing
- (Digital) Mailroom
- Information Management and Document Processing
- Intelligent Process Automation
- Omni-channel Output Processing

GDPR in a nutshell

With GDPR the EU is harmonizing data protection standards among member countries. Until now, each member state implemented its own version of the European Data Protection Directive of 1995 resulting in a variety of standards. GDPR came into force on 24 May 2016 giving organizations two years to implement and as of 25th May 2018 organizations have to comply. GDPR replaces national regulatory frameworks and enhances the rights of data subjects regarding their personal data, requiring:

- Lawfulness, fairness, transparency
- Integrity and confidentiality
- Purpose limitation, accuracy and data minimization
- Accountability

Personal data under GDPR is any information that relates to an identified or identifiable person. This person is called the "data subject". With GDPR the definition of personal data becomes broader covering a wide array of personal attributes, like names, contact data, online identities, ID and social security numbers, addresses, locations, IP addresses, as well as information that allows identification like genetic, biometric and medical data.

GDPR differentiates between Controllers and Processors. Controllers as well as Processors bear largely the same liabilities, whereas Processors act on behalf of Controllers. The Controller is an organization that defines means and purposes with regards to personal data. The Controller is primarily liable for data breaches. Typical Processors are managed services providers, cloud service providers, outsourcers, etc.

GDPR imposes obligations to correct, adjust and erase personal data on the request of a data subjects and report breaches within 72 hours. The use of personal data requires affirmative and clear consent from data subjects. Electronic copies of personal data must be provided to data subjects on request, including content, storage, location and purpose. Privacy and security must be built into systems, products and processes by design. It is required to maintain adequate documentation of data processing activities as well as implementing appropriate security standards (technical and organizational). Companies that process large amounts of personal data have to put in place mandatory internal controls in order to minimize privacy risks of data subjects and appoint a Data Protection Officer (DPO).