Data Protection

You Save It, You Delete It

GDPR brings legacy systems to the attention of data protection officers - technically as well as financially.

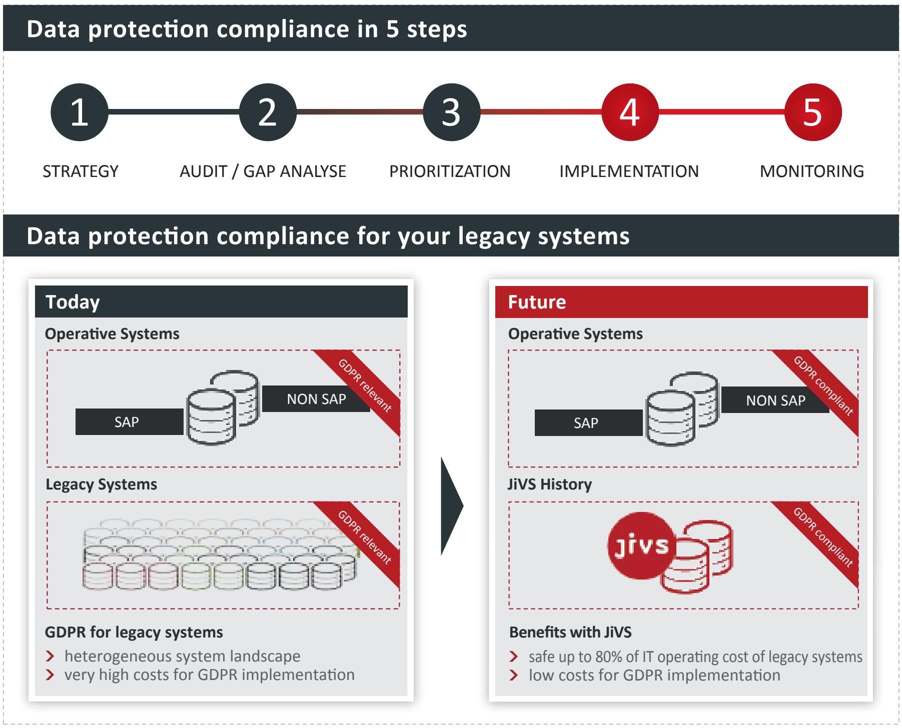
By Thomas Failer, Data Migration Services

The timer has finally run out. Today on May 25th, the transitional period for the EU's General Data Protection Regulation (GDPR) has ended. However, the technical and organizational measures necessary to fully comply with the requirements of the regulation still appear to be slow to find their way onto the priority list of IT managers. According to an IDC press release on October 2017: „44 percent of the organizations surveyed have not yet started any specific measures to meet the requirements; moreover, many still lack a holistic view of all personal data in the company.

„I can only confirm this situation from my numerous discussions with managing directors and board members over the past weeks and months," says Simon T. Oeschger, lawyer specializing in data protection law at the Swiss law firm Suffert, Neuenschwander and Partner. „Even the basic three questions - which data is stored where and who can access it - make many of my clients panic."

Thomas Failer,
Founder of Data Migration Services.

If you take a closer look, these observations are astonishing. Most of the principles of the new regulation have been part of earlier legislation for years in Europe, such as in the German Federal Data Protection Act. These include the principles of data economy, proportionality, earmarking and transparency. „These things have all been known for years, but the previous iterations of the regulation hardly qualify as anything more than toothless tigers," recalls Simon Oeschger from his experience. Even the new GDPR does not make it easy for those in charge to understand the explosive nature of the issue.



Data protection compliance in 5 steps

1 STRATEGY
2 AUDIT / GAP ANALYSE
3 PRIORITIZATION
4 IMPLEMENTATION
5 MONITORING

Data protection compliance for your legacy systems

Today
Operative Systems
SAP
NON SAP
GDPR relevant
Legacy Systems
GDPR relevant
GDPR for legacy systems
› heterogeneous system landscape
› very high costs for GDPR implementation

Future
Operative Systems
SAP
NON SAP
GDPR compliant
JiVS History
jivs
GDPR compliant
Benefits with JiVS
› safe up to 80% of IT operating cost of legacy systems
› low costs for GDPR implementation

Compliance in data protection in 5 steps.

No forest, just trees

According to Oeschger, the new regulation is extensive and, in many cases, not easily understandable to laymen. „It's the famous forest that you can't see for the trees," the lawyer sums up.

However, if one takes some of the new obligations from the regulations and looks at them more closely, their consequences quickly become apparent in all areas and levels of business: starting today, companies are obliged to provide information to customers and affected persons. They have the right to know what personal data the companies have stored, for what purpose the data was collected and whether storing the data was and still is permissible. In addition, companies must set up and maintain a register of purposes for which this data was collected and retained. If it turns out that too much data is stored, the companies must be able to specifically delete individual records.

„At this point at the latest, it will be clear that the new legislation is a task for the management and board members," explains Simon Oeschger. „Moreover, the protection of personal data must become part of general risk management, which has both technical and organizational consequences. Of course, digital knowhow becomes a need for company management - which must be acquired if necessary."

Nevertheless, according to Oeschger, there is no reason to panic. The most important thing is not to sit back and relax, because the deadline has not been met anyway. He recommends that a project is launched immediately to end the biggest data protection deficits and thus gradually become compliant with the new law, even if this can only be achieved after the deadline. Starting now also reduces legal risks: The draconian fines are imposed on a case-by-case basis and previous efforts made to comply with the new regulation are taken into account.

Five steps to a privacy culture

The first step on the way to proper digital risk management is data collection. The company must determine exactly which personal data is stored where. This is the prerequisite for step two, the GAP analysis. It is used to determine the main risks and thus, thirdly, their weighting, from which a prioritized list of the measures to be taken can be derived directly. According to Oeschger, the fourth step then is the implementation of the measures from this list. This includes processes as well as re-wording contracts and regular training of staff. The fifth step is to introduce and live a data protection culture based on iterative processes. „Corporate leaders must understand that data protection is not a one-off project," stresses Simon Oeschger. Rather, a data protection culture is characterized by iterative processes such as regular revisions and risk analyses.

Everything starts with taking stock of your data. However, companies must not stop at the productive systems because due to various storage obligations and periods, some of the personal data worthy of protection may be found in legacy systems. The rule of thumb here is: the larger a company, the higher the proportion of data in legacy systems.

The first Application Landscape Report by Capgemini revealed already in 2011 that half of the large companies expect to shut down every second legacy system. And in the 2014 report, respondents stated that this was not just a possibility, but a necessity. In many cases, this is due to the modernization of the ERP landscape in recent years, which has been accompanied by consolidation and centralization efforts at the same time. Put in simple terms: many different legacy systems are migrated to a few central live systems. However, only part of the data is transferred to the new environment.

With the upcoming migration to S/4 Hana, this wave of consolidation and centralization will continue to swell. Despite all the initial difficulties with the market launch and ongoing criticism from the SAP community, an online survey of 500 decision-makers in German-speaking countries conducted by the German-speaking SAP user group (DSAG) in early summer 2017 shows that almost 64 percent of the companies surveyed are now investing in SAP S/4 Hana in cloud and on-premise versions. By 2020, one third of existing SAP customers will switch to SAP's new software generation, and another 20 percent are already planning migration for the period after 2020.

It's the famous forest that you can't see for the trees.

Simon T. Oeschger, is a lawyer specialized on data protection at Swiss law firm Suffert, Neuenschwander und Partner, speaking about GDPR.

More than a simple necessity

One of the main reasons for consolidation and centralization is cost savings. Switching to new software generations costs a lot of money - money that is not readily available. According to a DSAG survey, IT budgets for 2017 grew by an average of almost five percent over the previous year.

Even such a significant increase will not be enough to provide IT departments with the financial resources they will need to digitize their businesses and their business models. The reason that no more funds are available is that around 80 percent of the total IT budget is used up by IT operations, while only 20 percent is available for investments in innovations. Surveys have shown this result time and time again. 70 percent of this is often due to the cost of legacy systems alone. In contrast, a division of 60 percent for IT operations and 40 percent for innovations would be ideal on a permanent basis.

However, this goal can only be met if the old systems are permanently switched off. „This is precisely where the intersection between data protection and business management lies," stresses Simon Oeschger. „Because by taking stock in step one, the old systems come back into focus. Companies simply cannot afford to put them back into operation just because of the General Data Protection Regulation."

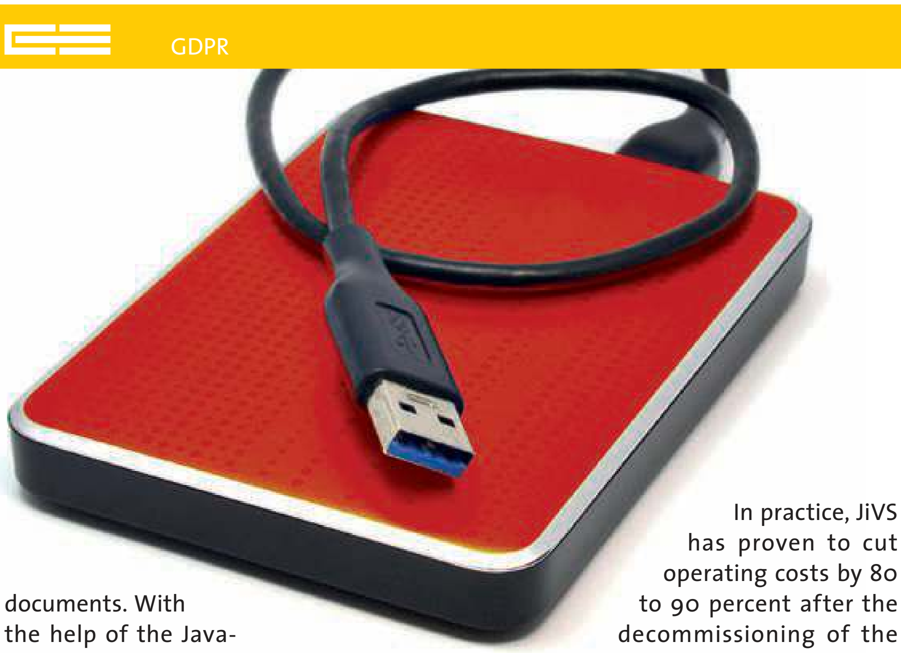
In addition to cost considerations, however, there are also technical limitations. For example, many legacy systems do not offer any possibility to delete specific data records. Retrofitting them is also not possible in many cases, because at least some of these systems have already been taken out of the manufacturer's maintenance or are in read-only operation.

Historicization instead of archiving

What is needed is a change of perspective. Often one problem turns out to be the solution for another. If the new regulation makes it necessary, but too expensive, to continue operating legacy systems or even to get them out of hibernation; if also, on the other hand, there is not enough budget for the modernization of IT, but modern systems are needed, then there is only one way out: to end the expensive operation of legacy systems and thereby permanently cut the associated operational cost. This is where compliance becomes much more than a simple necessity. However, a new approach to data management is a must. This new approach applies not only to data, but also to documents containing personal data.

Moreover, data and documents do not exist on their own, but need to be put into a specific business context. To be able to decide and justify whether personal information was collected and stored in accordance to the new regulation, this context must also be preserved if one wants to switch off legacy systems in the long term. It's not about archiving, but about managing the entire life cycle of information. Regarding legacy data and documents, it therefore makes more sense to speak of historicization.

As with the modernization of IT systems environments, the principle of standardization also applies to the historicization. This is a core feature of JiVS, a central solution for managing historical data and



documents. With the help of the Java-based platform and its component „JiVS History for GDPR“, the information transferred from decommissioned legacy systems can be documented with retention periods and deleted irretrievably and automatically after the legal retention periods have expired. In addition, this comprehensive „retention management“ allows automatic deletion to be suspended in exceptional cases such as ongoing court proceedings at the level of individual data records and documents in the sense of a so-called legal hold.

In practice, JiVS has proven to cut operating costs by 80 to 90 percent after the decommissioning of the old systems. With the remaining 10 to 20 percent, the legacy data, including SAP business logic, can continue to be used for compliance reasons. This also offers a unique opportunity to clean up the existing records and especially the master data. Especially this last adjustment is decisive for the successful move to S/4 Hana for cost reasons. Moreover, this applies equally and without restriction to compliance with the requirements of GDPR in order to comply with the principle of data economy.

Conclusion

Existing SAP customers are in a dilemma between budget constraints on the one hand and the pressure to innovate and compliance requirements in accordance with the General Data Protection Regulation on the other. The closure of old systems and archives is the way out of this impasse. Intelligent platforms reduce the number of operational SAP systems and the amount of information they contain. JiVS creates the necessary financial freedom for the new generation of SAP software and makes the IT landscapes of existing customers weatherproof for current and future compliance requirements. Then you can start deleting.

www.jivs.com