GDPR for Non-Production SAP Environments

ABSOFT
SOLUTIONS FOR BUSINESS

SAP Silver Partner

GDPR FOR NON-PRODUCTION SAP ENVIRONMENTS

BY DON VALENTINE

SITUATION

In the lead up to GDPR on May 25th, much thought had been given to what data needs to be protected, retained, deleted and managed in SAP Production environments. However, GDPR Applies to Non-Production SAP Environments too!

There are plenty of articles and blogs, quite rightly, considering the pervasion of sensitive personal data throughout a Production SAP environment:

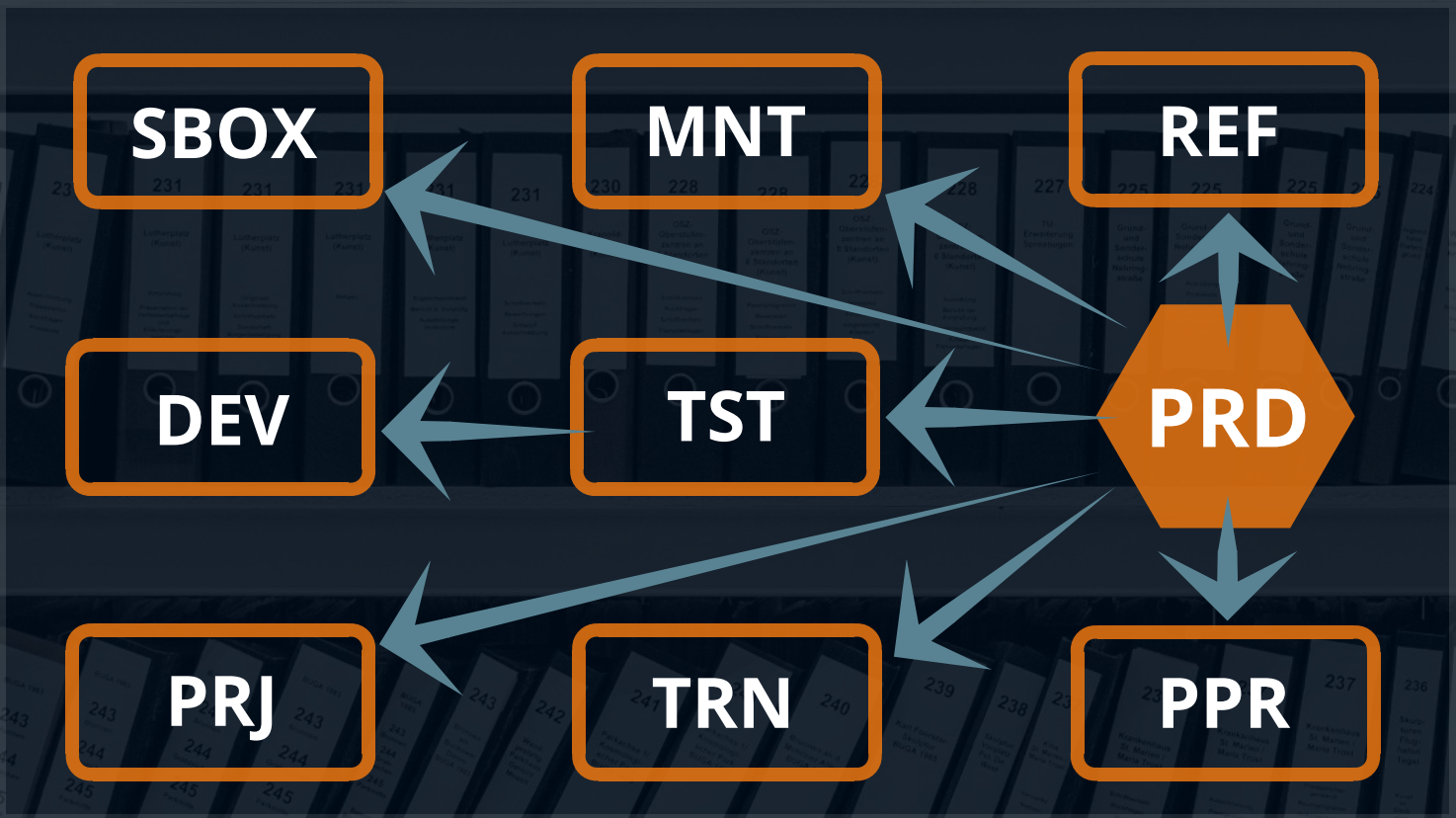
- employee data that is not just in the HR or Payroll modules but also in Finance Accounts Payables for expense payment purposes;
- employee data that is in approval workflow constructs;
- employee and payroll data that is perhaps in external pension interface files.

There is much to consider in terms of system, process, data and people implications to ensure that your SAP Production system and data management protocols are GDPR compliant.

SITUATION

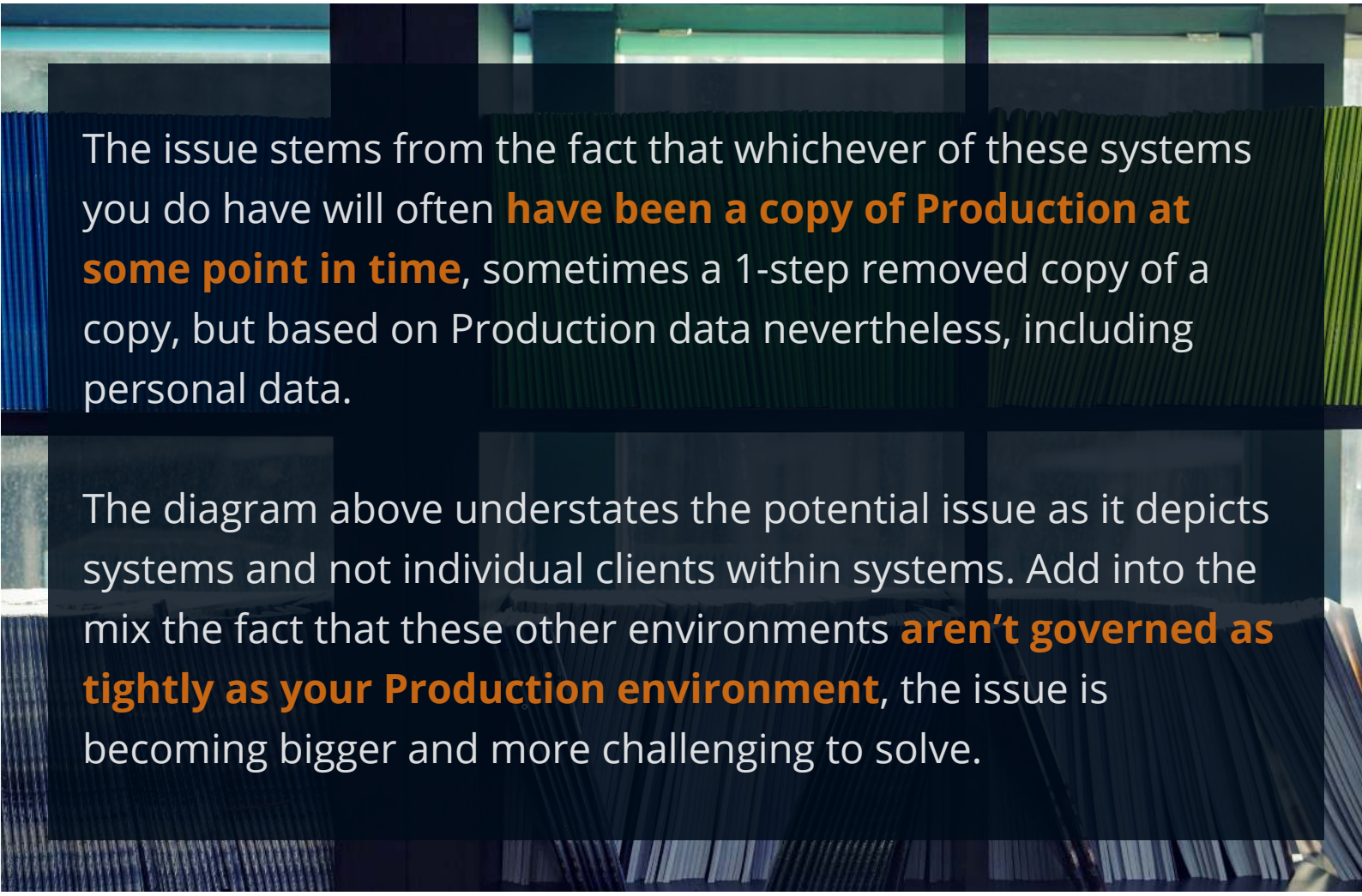
Less heralded, and perhaps attracting less attention, has been the fact that this **same sensitive personal data is often available in a host of non-Production SAP instances.**

Not every SAP customer has all the instances portrayed in the diagram below – but you will have some of them:



1. **PRD** - Production
2. **TST** - a.k.a QAS - where we test fixes/enhancements
3. **DEV** - where we develop fixes and new solutions
4. **SBOX** - where we play and prototype solutions
5. **REF** - a reference SAP system keeps for historical data retention purposes often after a divestment, a franchise change or a change of ERP
6. **TRN** - a training environment
7. **PRN** - a Payroll Parallel Run environment
8. **MNT** - a maintenance environment created for shipping emergency fixes during Projects
9. **PRJ** - Dedicated project environments created for significant projects - keeping them away from the route-to-live operational support systems during development

SITUATION



The issue stems from the fact that whichever of these systems you do have will often **have been a copy of Production at some point in time**, sometimes a 1-step removed copy of a copy, but based on Production data nevertheless, including personal data.

The diagram above understates the potential issue as it depicts systems and not individual clients within systems. Add into the mix the fact that these other environments **aren't governed as tightly as your Production environment**, the issue is becoming bigger and more challenging to solve.

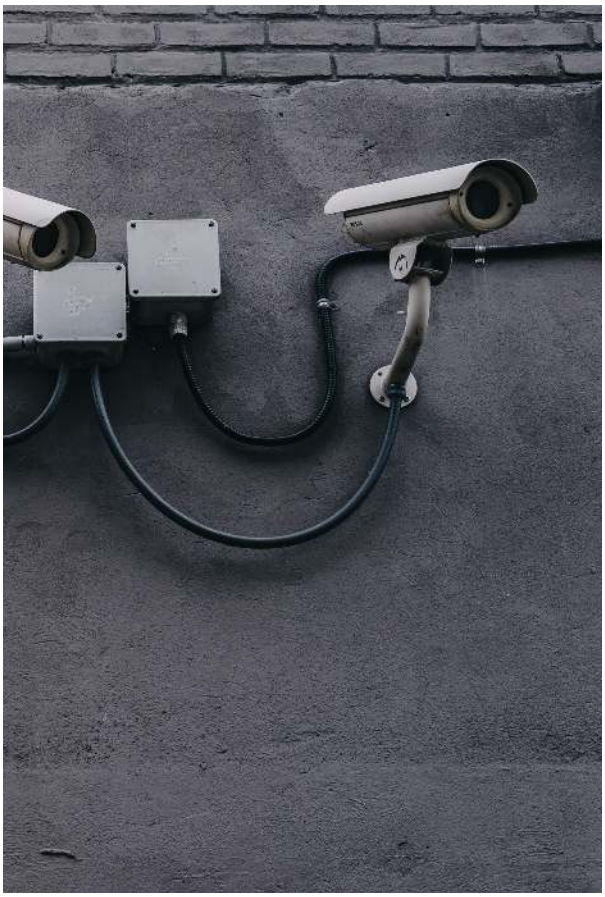
The non-Production environments also tend to be the domain of a very different set of "techy" communities.

They usually comprise of **business users that use the Production environment**; configurers, developers and technical resources from your own organisation and from 3rd parties will all be active in them.

Furthermore, in these non-Production environments, these "techies" tend to **be equipped with security privileges which may be sensitive to configuration and development related activities** but pay little or no heed to business data related security constructs that safeguard your production data.

IMPACT

The result of the above is that whilst organisations may have developed GDPR processes, procedures and instituted the organisational updates associated with GDPR for SAP Production systems, **they may be equally or more exposed to GDPR non-compliance in their non-Production systems.**



The potential penalties for GDPR non-compliance have been well publicised but to reiterate, the fines can be up to €20 million or 4% of annual turnover of the previous year, whichever is higher.

SOLUTION

PURPOSE DUE DILIGENCE

As with most legislative changes impacting IT systems, due diligence is involved in scoping what needs to be done to make these non-Production systems GDPR compliant.

One of the key precepts of GDPR is a piece of due-diligence called PURPOSE, in which we need to consider and document the purpose to which data is processed in a particular context.

This PURPOSE due-diligence can be a very useful exercise in addressing, or at least clarifying, the types of solutions that should be deployed to address prevailing GDPR concerns in non-Production system/Production data systems. If you consider each system and its purpose, and in turn "hold their feet to the GDPR fire", you will probably identify three main system categories:

1. Systems in which personal data needs to be identifiable/non-anonymised, e.g. Production (as a given), Reference systems and Payroll Parallel Run systems

2. Systems in which the personal data does not need to be identifiable so it can be anonymised, e.g. potentially Development, Test, Training, Sandbox, Project (excluding HR Projects), Maintenance systems

3. **Systems which may be appropriate for "pseudonymization" -** a privacy-enhancing technique where data which could lead to direct identification is held separately and securely from processed data. To be able to turn anonymised source data into an identifiable data you need access to another separate piece of information to decode it, like in a spy thriller where they need to have both parts of the postcard to decrypt the data.

TECHNICAL SOLUTIONS

DATA LIFECYCLE MANAGEMENT SOLUTIONS

In the previous section of this article, I outlined three categories of technical solutions which might be deployed to help address GDPR issues in your non-Production SAP environments:

1. Data Lifecycle Management solutions

2. Obfuscation or Masking solutions

3. "Pseudonymization" solutions.

In this article, I won't be covering category 3 solutions due their "special case" status and will concentrate on the more prevalent use cases and therefore solutions 1 and 2 above.

1. Data Lifecycle Management solutions will typically group personal data related data objects and records into groups with each data group having a distinct set of event triggers (which start/stop the clock ticking) and a staged lifecycle which will typically involve time related reductions in levels and ease of access to the data potentially leading up to eventual data deletion.

Often the secret of defining the right groups of data and the right lifecycle profiles is to **balance the rights of the individual with the legal and statutory demands that are placed on the organisation.**

As might be imagined, obsolete address related data as one potential data group would have a very different GDPR profile/lifecycle than say a payroll results, bank account or basic salary related data group due to their levels of sensitivity and legislative reporting demands.

TECHNICAL SOLUTIONS

DATA LIFECYCLE MANAGEMENT SOLUTIONS

These different data groupings and their associated event triggers and lifecycle rules **need to be configurable**, partly because hard coding is never good, but also to retain the flexibility to adapt to changing requirements. Configuration of course starts in a Development environment or Sandbox and is then promoted via transports into the various environments implicated.

Data Lifecycle Management solutions involve coordinated development across multiple dimensions.
System solutions must be designed, built, implemented and people need to be trained in new processes and/or procedures. Cut-over plans also need to be developed as part of the deployment.

Implementation of Data Management Solutions involves serious planning and will require a reasonable associated budget. It is not a days or weeks effort, it will take months.

Easier, quicker and less costly to implement are the more technically oriented **obfuscation/masking solutions:**

TECHNICAL SOLUTIONS

OBFUSCATION / MASKING SOLUTIONS

As described previously, if you consider the PURPOSE to which identifiable personal data is put in many of your non-Production SAP environments Development (Dev), Sandbox (SBX) and Training (TRN), you will identify that there is no need for that data be real/actual data.

Anonymising that data would have detrimental impact to the PURPOSE to which that data is put. This type of scenario is where obfuscation/masking solutions come into play.

Of course, we need to define up-front the data fields that should be anonymised and how we want them to be anonymised, typically with scrambled values or blanks, but we have done the hard work by performing that due diligence and configuring those fields into your chosen anonymisation solution.

The anonymisation programs will run as scheduled, typically after a system copy from a Production (or Production based) system and will ensure that we no longer have identifiable personal data represented in our system.

At risk of over-simplifying, there are cases where you will need to consider aspects such as formatting, foreign key relationships and other matters. As an example of this, we would typically anonymise National Insurance (NI) numbers but in doing so we need to respect the format of NI numbering conventions to prevent the system failing on validation checks. That being said, there is no doubt that obfuscation/masking solutions are easier to design and configure and faster to implement than the data lifecycle management solutions.

RECOMMENDATION

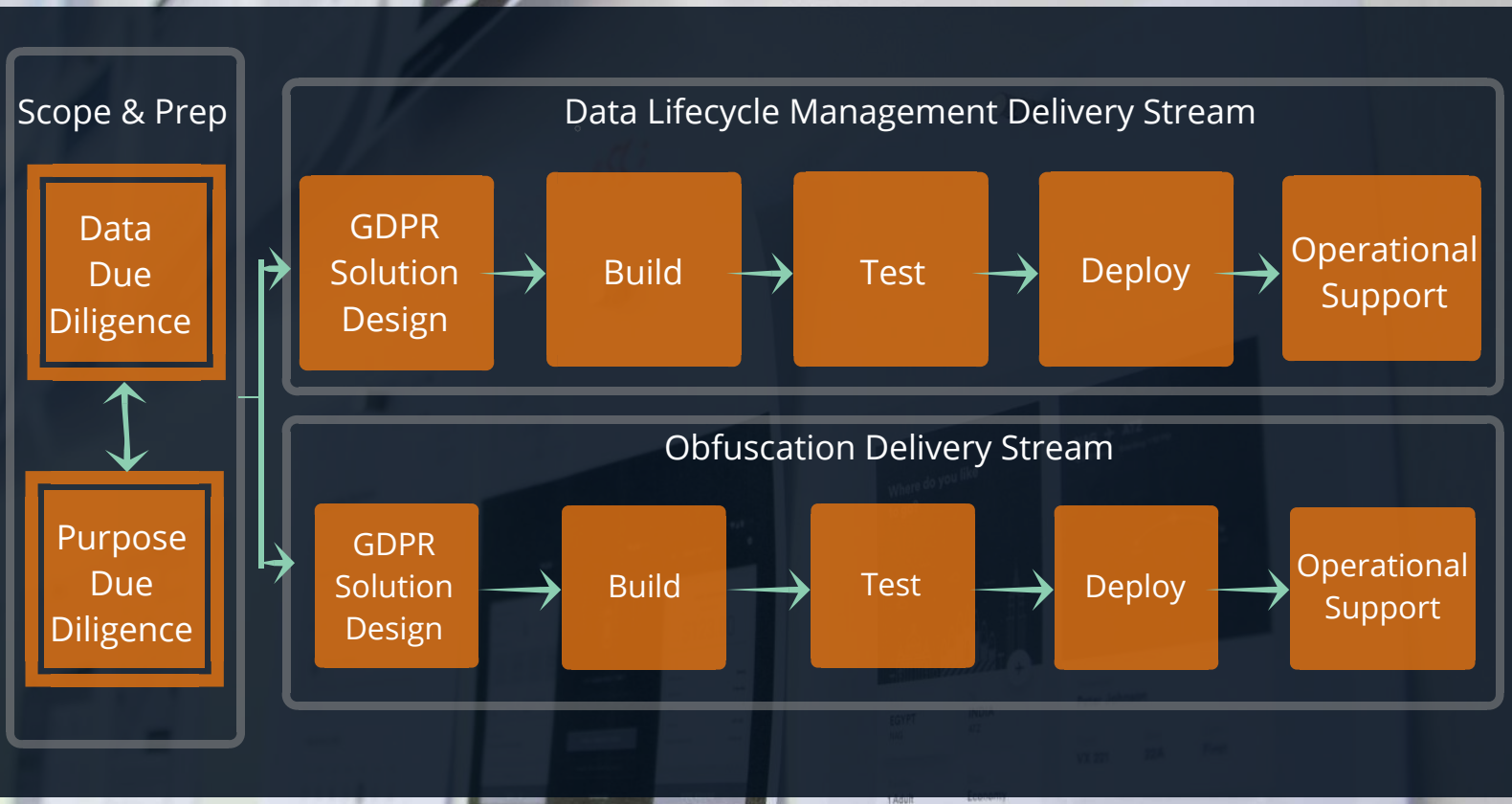
FOUR KEY TAKE-AWAYS

1.

Don't forget your non-Production SAP environments – they may well be more exposed to GDPR risks than Production.

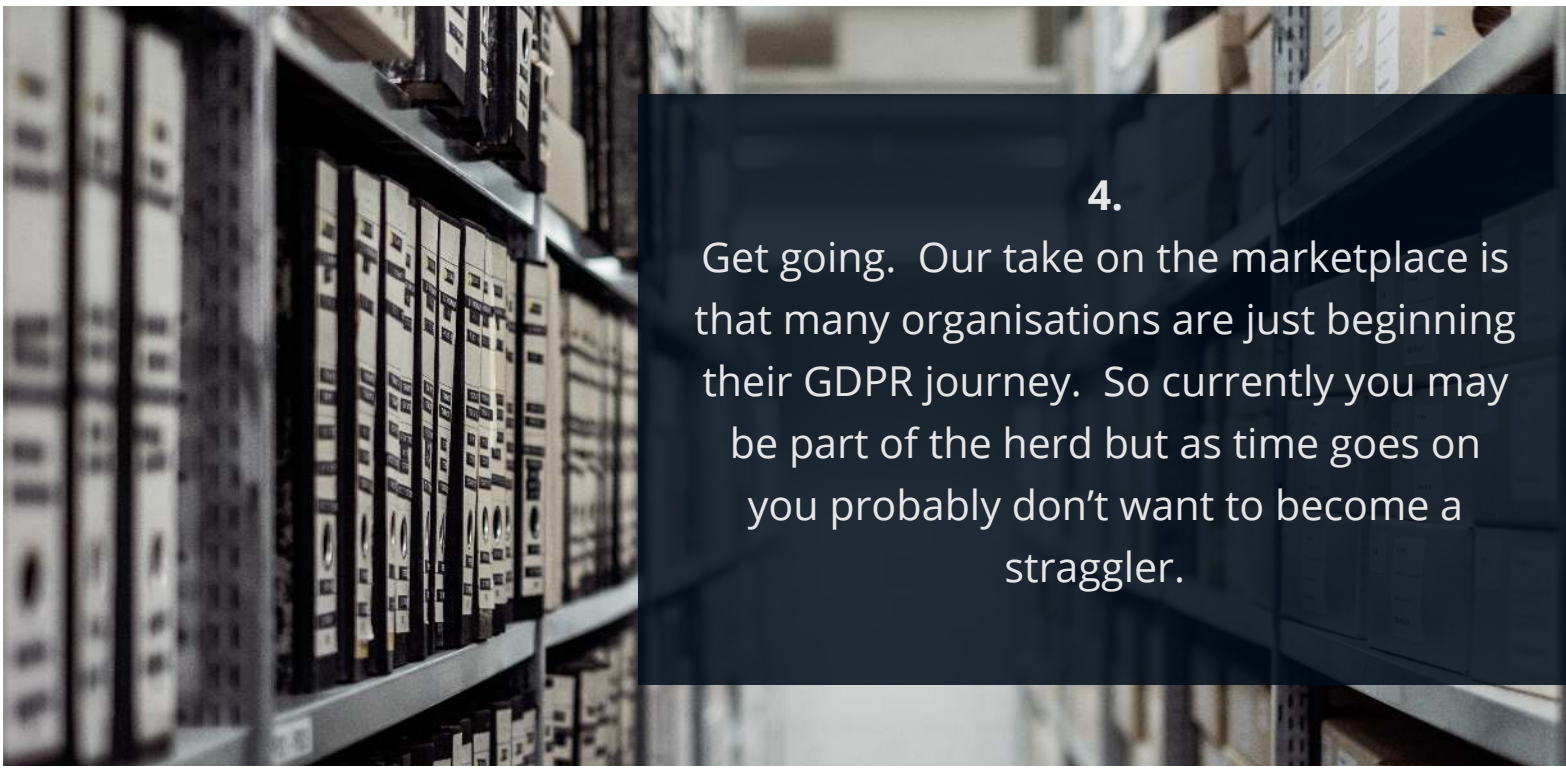
2.

There is no substitute for up-front due diligence. You need to identify and scope your GDPR related personal data and you need to understand where that data is held and for what purpose in your full SAP landscape. These Due Diligence efforts should set the scene for your GDPR Delivery Streams.



3.

Once you have done your due diligence, I would suggest that you separate your GDPR Design, Build, Test and Deploy efforts into the two main streams of Obfuscation and Data Lifecycle Management due to their palpable differences in scope, timeframe, cost and organisational impact.



4.

Get going. Our take on the marketplace is that many organisations are just beginning their GDPR journey. So currently you may be part of the herd but as time goes on you probably don't want to become a straggler.

ABOUT ABSOFT

Absoft, SAP Partner and SAP Value-Added Re-Seller (VAR), has been specialising in SAP® since 1991, uniquely combining business process and SAP expertise to deliver best practice solutions in implementation, development and support of SAP solutions.

In their words, our clients value our **"flexibility, willingness to go the extra mile, full transparency, being proactive in suggesting and providing the right solution, not just overhead".** Eighty percent of our business is from repeat customers.

+44 (0)1224 707088
info@absoft.co.uk

www.absoft.co.uk