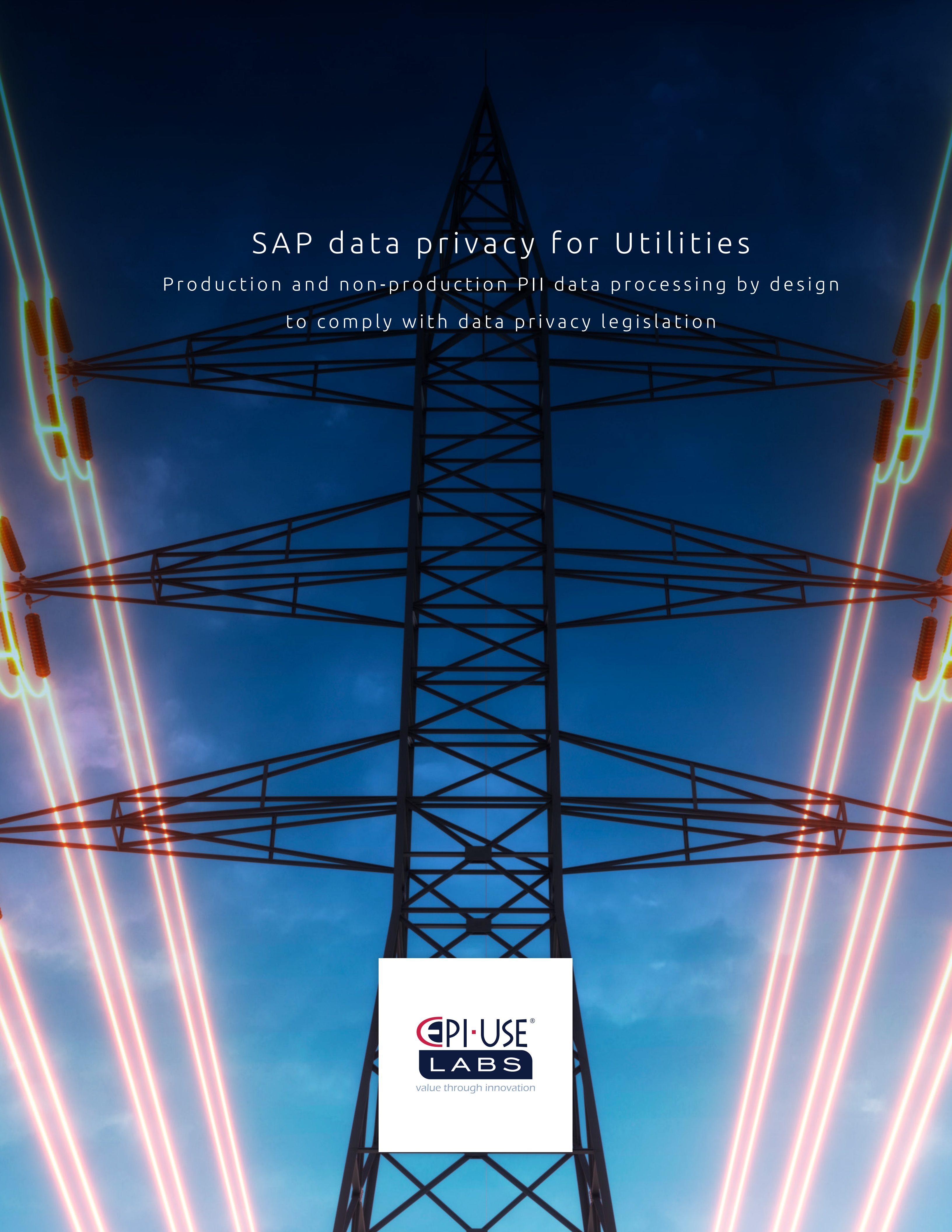
SAP data privacy for Utilities

Production and non-production PII data processing by design to comply with data privacy legislation



EPI-USE® LABS

value through innovation

Why is privacy such a concern for Utilities?

Unlike many industries, to be able to perform the most basic of Utility industry functions – producing a bill for supply to a property – requires you to know a huge amount of Personally Identifiable Information (PII). Since each Utility company provides a service to multiple millions of customers, and is likely to have copies of this same data in non-production landscapes, this adds up to a massive data liability.

Around the world, we are seeing the advent of privacy laws now with:

- Five US state legislations and a federal bill under review
- GDPR covering European citizens
- POPIA in South Africa
- LGPD in Brazil
- PIPL in China.

Although each law is different, similar tenets are found, requiring:

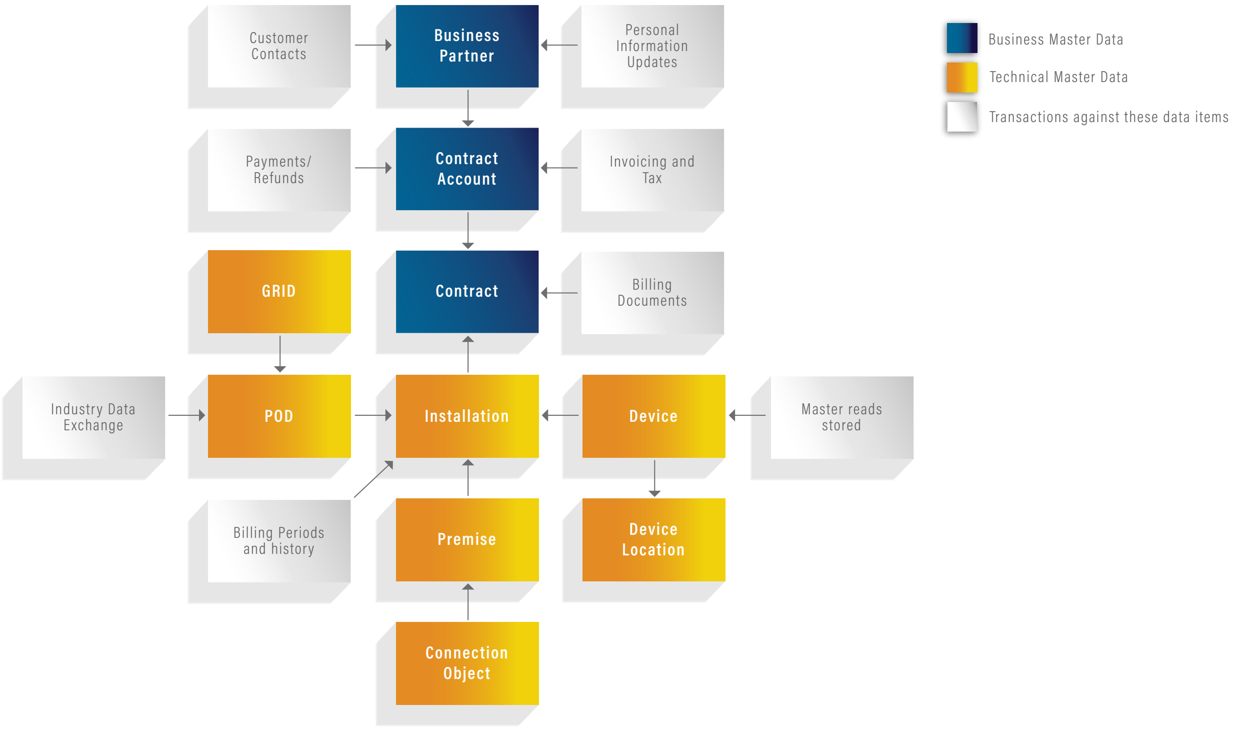
- the proactive removal of data
- restrictions on transmission of data, and
- informed consent on the use of personal data.

The challenges of SAP IS-U

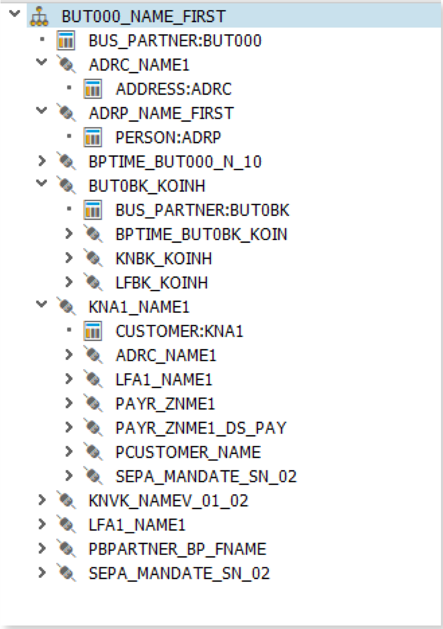
Most SAP IS-U customers have seen a similar image to this, showing the difference between Business Master Data and Technical Master data. The same technical Premise and Installation are used for multiple Business Partners.

The largest issue for handling the removal of data comes when you consider billing. As the installation remains static between multiple accounts, the billing process expects a full billing history at all times. If a missing billing period is found in an old accounting period, this will still affect the most recent bill you are trying to produce.

With this backdrop, when you consider the now legal requirement to remove PII data from your system, there is a huge challenge. Traditional archive deletion will not work, as it will create these inconsistencies on the shared technical master data.



So, what's the solution?



- BUT000_NAME_FIRST
  - BUS_PARTNER:BUT000
  - ADRC_NAME1
    - ADDRESS:ADRC
  - ADRP_NAME_FIRST
    - PERSON:ADRP
  - BPTIME_BUT000_N_10
  - BUT0BK_KOINH
    - BUS_PARTNER:BUT0BK
    - BPTIME_BUT0BK_KOIN
    - KNBK_KOINH
    - LFBK_KOINH
  - KNA1_NAME1
    - CUSTOMER:KNA1
    - ADRC_NAME1
    - LFA1_NAME1
    - PAYR_ZNME1
    - PAYR_ZNME1_DS_PAY
    - PCUSTOMER_NAME
    - SEPA_MANDATE_SN_02
  - KNVK_NAMEV_01_02
  - LFA1_NAME1
  - PBPARTNER_BP_FNAME
  - SEPA_MANDATE_SN_02

EPI-USE Labs' Data Sync Manager™ (DSM) for Utilities contains a complete mapping of the standard SAP IS-U data model including integrations between systems and objects. With the advent of GDPR in 2018, Data Sync Manager was enhanced to have a field-level mapping of PII data within this model. As such, the mapping of a simple name field in table BUT000 considers the relationship between IS-U and CRM, internal assignment to Address data, Customer data, and much more. Using this mapping, the DSM Data Secure™ solution allows for the creation of context-specific rules of data anonymization.
Data scrambling can be interfaced directly with the selective data copy provided by DSM Client Sync™ and Object Sync™, or run in place following a traditional data refresh. However, through the integrated approach, you can:

- minimize the amount of data transferred from production
- enforce scrambling on exit (the PII never leaves the production instance during transfer), and
- provision test data on demand of production quality, without the PII data risk.

That will take care of non-production for you – often a key concern as the non-production environment regularly has lower access control and higher data portability (offshore access to data). However, this doesn't address the production risk and issues with archiving already described.

The EPI-USE Labs' Data Privacy Suite for SAP® solutions was specifically designed for use in production to avoid these issues.

The suite consists of four components:

- DSM Data Secure™ (as above)
- DSM Data Disclose™: Uses the field-level mapping of Data Sync Manager to search and identify the PII data held in connected systems for the same data subject, collating that information, and presenting it into a password-protected, encrypted PDF. Data Disclose simplifies the Subject Access Request (SAR) process.
- DSM Data Redact™: Provides surgical removal of PII data from the SAP data model, without requiring complete deletion or archiving. We will remove the Name, Bank Details, Telephone number, and so on from a Business Partner and its linked data objects. As such, the referential integrity, billing periods, meter read history, and business and technical master data relationships can all remain without PII.
- DSM Data Retain™: Automated queries to check alternate payer relationships, Contract Move-Outs, account balances, dunning stages, and so on, to proactively identify data which has not been processed for more than X years. Those records can be submitted to Data Redact for data removal, providing proactive PII data management which understands the intricacies of SAP IS-U.

Combining DSM for Utilities and the Data Privacy Suite, you can confidently approach your compliancy audits in the knowledge that you have production and non-production – reactive and proactive – PII data processing by design.

Where should I start?

EPI-USE Labs has completed multiple privacy projects around the globe, and there is a common question raised from most of the Data Protection Officers we work with:

"What is my PII Data Risk – how do I quantify it and build a business case?"

EPI-USE LABS
Data privacy workshop and system analysis
Prepared by EPI-USE Labs for

The answer in SAP is never simple, and in IS-U, it's even less so.
For example, every address that is supplied has the same address stored at least four times just in the standard model: once for the Business Partner, once as the POD/Connection Object address, once as the Premise, and once for the person record. Without domain knowledge of the specific IS-U solution, it would be impossible to find and handle all of these related data items.

So that is where we start. EPI-USE Labs has been handling the SAP data model for the over 20 years and has built the mapping already mentioned. With our understanding of the SAP building blocks, we have built specific discovery technology leveraging this IP to be able to search and identify all the related custom tables and fields which have been built, that have related PII data.

As such, using this report, we are able to help build a detailed data map of your PII data and show you where the Names, Bank Details, Email addresses and more are stored in your SAP system. With the architecture and data relationships/flow, business requirements and technical options are clearly documented, so you can build your business case with ease.

> *"With the EPI-USE Labs' approach, we can anonymize and redact sensitive data rather than archive, meaning business transactions may stay in the system without being related to an identifiable individual. Now, when starting projects, we have frameworks for how to do information sensitivity and risk analyses, and from there come the requirements on the IT side, including the sensitivity of data – the complete information security perspective."*
>
> Richard Wenell, Head of IT department, JM

> *"Thanks to Data Secure, we can anonymize all sensitive SAP HCM data, such as employee-related data, in a very short time. The biggest advantage of Data Disclose is that data integrity is guaranteed; customers' sensitive data is anonymized but all orders and items sold are still accessible. All test systems stay fully functional, and test orders are still editable."*
>
> Malte Podszus, Consultant FI/CO/HR, MAPA GmbH