White Paper

Mastering the GDPR with Enterprise Architecture

Contents

INTRODUCTION

Rising levels of worldwide digitalization and the increasing use of social networks, cloud computing, and other online services have made the need for modern data protection regulations ever more pressing. On May 25, 2018, the wait will finally be over: that is when the new EU General Data Protection Regulation (GDPR), designed to reform data protection in Europe comes into force. Any company that operates within the EU and processes personal data will have to adhere to this regulation in the future. The GDPR has numerous advantages due to the standardization it entails, but for many businesses, the new regulation is both a blessing and a curse. A current Gartner study shows that around 50 percent of all organizations will not fully meet the new EU General Data Protection Regulation by the end of 2018.[1] That may become costly for business owners, as there are heavy penalties for failing to comply with the GDPR. In order to ensure that your company is successfully prepared for integrating the GDPR, you will need exact information on which data your company stores and processes. It is precisely the quality and complexity of their data that may become data protection pitfalls for companies, as they often do not know which personal data are processed where.

In those cases, a good Enterprise Architect (EA) can be the key to compliance, assisting the data protection officer in implementing the GDPR and giving important insights into the corporate IT landscape.

[1] Gartner 2016: https://www.gartner.com/doc/reprints?id=1-3V903Y9&ct=170309&st=sg

Close cooperation between a company's EA and their data protection officer is, therefore, a fundamental requirement.

The countdown has begun – there is not much time until the new regulation comes into force on May 25, 2018. How well do you handle data protection issues? This white paper highlights all the stumbling blocks associated with the GDPR and shows you how Enterprise Architecture can help you overcome them.

THE GDPR AND WHAT IT MEANS FOR YOUR COMPANY

Companies have to work through a large number of complicated steps in order to become fully compliant with the new EU-GDPR. Significant additional expense is to be expected on the part of the organizations. According to a current Ponemon study, more than one-third of surveyed German companies said they had not yet taken any steps towards ensuring GDPR compliance.[2] Equally concerning is the fact that only 38 percent of global businesses have a specific implementation plan.[3] This is due among other things to the imprecise wording of the data protection regulation, which is causing confusion and problems in implementation. Some degree of legal uncertainty is therefore to be expected in the early stages.

The new EU regulation

After lengthy negotiations, the new legal basis for data protection in the EU was adopted on May 25, 2016. With the introduction of the new EU-GDPR, there will be only one applicable law for all 28 EU member states. The aims of the regulation are on the one hand to protect the fundamental rights and freedoms of natural persons and on the other hand to enshrine their right to protection of their personal data as well as the free movement of these data (see Art. 1 GDPR). The new regulation will come fully into force on May 25, 2018, and thus looms increasingly large. Companies must act now, as numerous measures are required to become compliant, and breaches of the GDPR or failure to meet the deadline can be costly for them.

What is personal data?

According to EU Directive 95/46/EC, personal data is "any information relating to an identified or identifiable natural person [...] who can be identified, directly or indirectly [...]" (see Art. 2 of Directive 95/46/EC). Data such as name, address, e-mail address, ID card number, IP address and information provided on gender, title, height, hair color etc. is therefore personal data. Information considered especially sensitive includes data on origin, politics, health, religion, ethnicity, trade union membership or sexuality (see section 3 par. 9 of the German Data Protection Act) is also considered personal data.

To whom does the law apply?

The GDPR states fundamentally that it applies to any person in an organization (e.g. legal person, public authority, institute etc.) that operates within the EU and processes personal data. The new regulation moreover also applies to non-European companies if they operate within the EU, and to data processing companies regardless of whether the data are processed within the EU (see Art. 3 GDPR). In the future, the marketplace location principle will pertain: the new regulation applies if the service is aimed at a specific market within the EU or the data are processed on behalf of persons in the EU.

Strictly speaking, every company is affected, as organizations process sensitive data in the workplace almost every day: bank account details, telephone numbers, contracts, pay scales, etc. Companies are therefore responsible for the safety of their data and for that of the personal data of their employees and customers.

[2] Computerwoche: https://www.computerwoche.de/a/compliance-ist-nur-der-anfang,3330661?tap=7e2bccd20d41c66e4e860c3c78ec6fac

[3] SearchSecurity: http://www.searchsecurity.de/news/450419077/EU-DSGVO-US-Unternehmen-besser-vorbereitet-als-europaeische-Firmen?

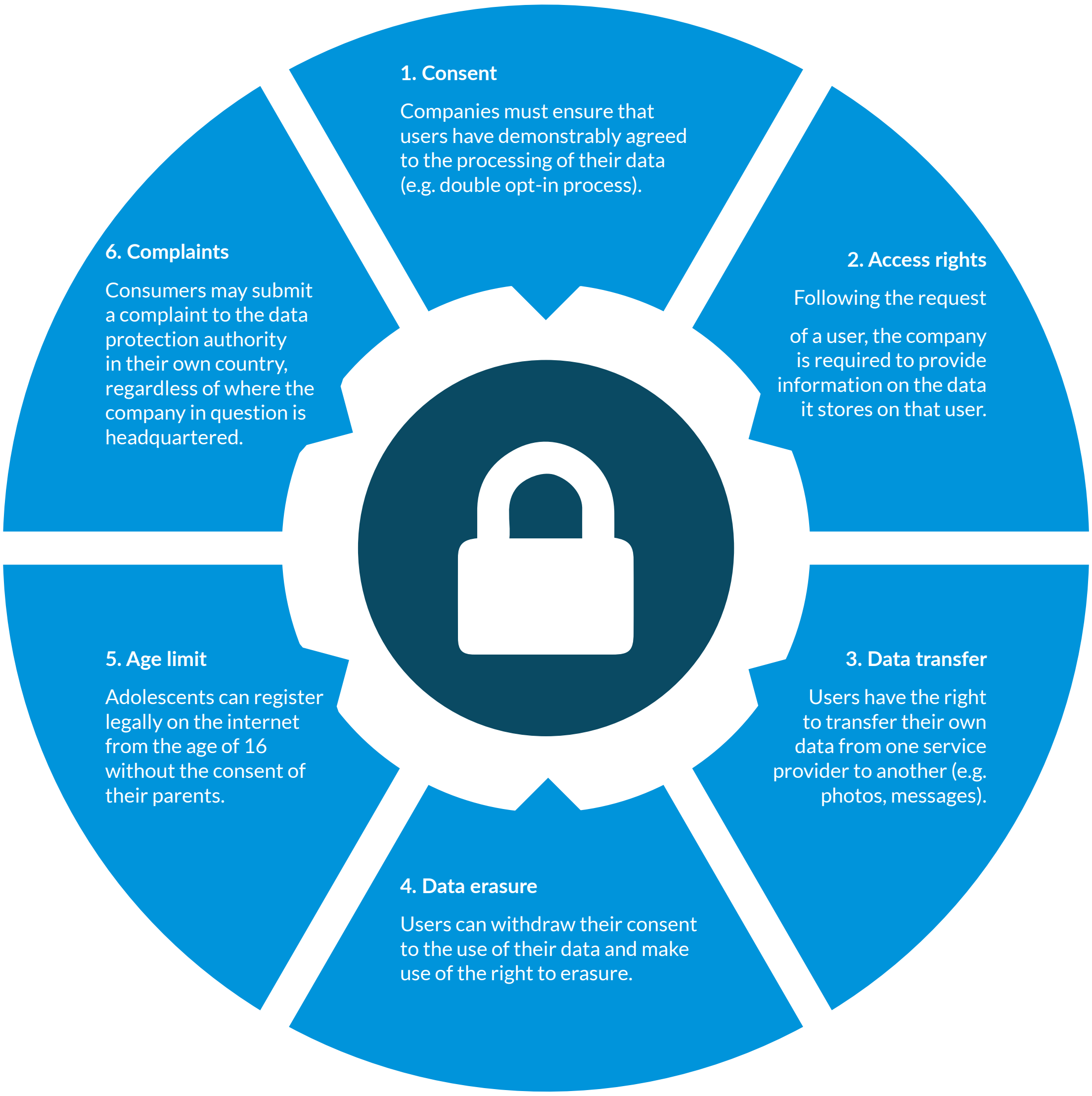
What is changing?

The GDPR will standardize data protection law across Europe in order to give individuals better control of their data. Accordingly, the same data protection laws will apply in all EU member states in future; data protection "gray areas" will no longer exist in Europe. A major challenge for businesses is doubtless the implementation of data subjects' rights, that is, the rights of the people whose data they are storing (see fig. 1).

The new EU regulation thus brings new obligations for businesses. Less than half of all companies around the world have a concrete plan for implementing these obligations.[4] There are six major areas that companies will have to consider[5]:

1. Data protection through technology (Art. 25 GDPR)

Companies are required to define internal strategies and initiate steps to ensure data protection through technology (by design) and as a standard approach (by default). Possible measures include minimizing and pseudonymizing the processing of personal data. Furthermore, transparency must be established with regard to the functions and the processing of personal



1. Consent

Companies must ensure that users have demonstrably agreed to the processing of their data (e.g. double opt-in process).

2. Access rights

Following the request

of a user, the company is required to provide information on the data it stores on that user.

3. Data transfer

Users have the right to transfer their own data from one service provider to another (e.g. photos, messages).

4. Data erasure

Users can withdraw their consent to the use of their data and make use of the right to erasure.

5. Age limit

Adolescents can register legally on the internet from the age of 16 without the consent of their parents.

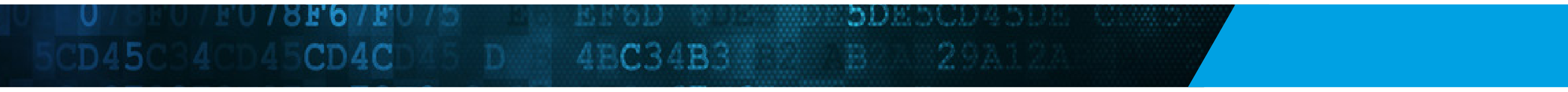
6. Complaints

Consumers may submit a complaint to the data protection authority in their own country, regardless of where the company in question is headquartered.

Fig. 1: What is changing – user rights

[4] SearchSecurity: http://www.searchsecurity.de/news/450419077/EU-DSGVO-US-Unternehmen-besser-vorbereitet-als-europaeische-Firmen?

[5] DSGVO: https://dsgvo-gesetz.de



data, data subjects must be allowed to monitor the processing of their data, and the persons responsible for processing must be enabled to create and enhance security functions.

What measures have you already been implemented, and what measures are still needed?

2. Accountability (Art. 5 GDPR)

Companies are required to ensure and demonstrate adherence to data protection regulations, for example through certification.

Has your company introduced a data protection program, and is your company able to demonstrate that it meets GDPR requirements?

3. Notification requirements (Art. 33 GDPR)

Companies are required to report data breaches (e.g. through hacking attacks) immediately, within 72 hours, to the competent supervisory authority and the affected data subjects. Failure to do so may lead to fines of up to 20 million euros or 4% of the company's global annual turnover.

Are corresponding processes implemented in your company to meet this requirement in a timely manner?

4. Data protection officer (Art. 37–39 GDPR)

It will become mandatory for all companies in Europe to appoint a data protection officer. According to the GDPR, the data protection officer's responsibilities include informing and advising the data controller or processor and the employees who carry out processing; monitoring compliance with the GDPR and national data protection provisions; awareness-raising and training; providing advice as regards the data protection impact assessment and monitoring its performance; and cooperating with the supervisory authority.

Do you know who is your company's data protection officer?

5. Data protection impact assessment (DPIA, Art. 35 GDPR)

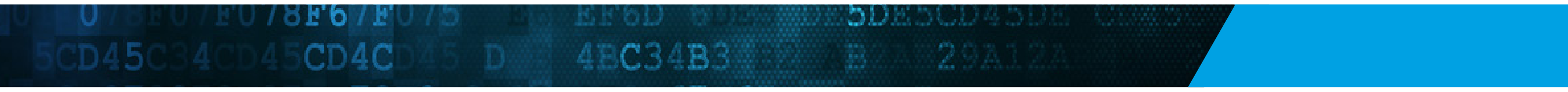
A DPIA must be performed "[...] where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons [...]". The data protection officer analyzes the risks of the process together with the technology owners and then submits a declaration on the legality of the data processing.

Does your company regularly conduct data protection impact assessments for new technologies?

6. Penalties and fines (Art. 83–84 GDPR)

More severe fines and penalties are designed to deter companies from infringing against data protection regulations and to make companies more aware of the fact that offenses also violate the EU Charter of Fundamental Rights. Fines of up to 20 million euros or, for companies, up to 4% of annual turnover in the previous business year may be levied. Other penalties, such as seizure of profits, injunctions to end infringements, and permanent prohibition of data processing may also be imposed.

Have you invested appropriately in your IT landscape in order to avoid such fines?



ENTERPRISE ARCHITECTS & THE GDPR

The players

Although the data protection officer is the main person responsible for compliance with and implementation of the GDPR, Enterprise Architects (EAs) are ideally placed to play a pivotal role in this implementation.

EAs offer data protection officers insights into all processes, applications and data, and provide the necessary information on data objects, data flows and responsibilities. Enterprise Architects also point out potential risks and compliance breaches. They can help those responsible for a technology (e.g. for an application, an interface or a data object) to identify technology risks and prepare preventative measures. This is especially relevant with regard to the data protection impact assessment (DPIA), which must be performed before a new technology is deployed. As an Enterprise Architect you should ensure that you communicate with the responsible data protection officer and coordinate all necessary steps.

The role of EA

Successfully preparing your business for integrating the GDPR will require a lot of architectural work. A study found that companies consider ensuring data quality (73%) and handling data complexity (67%) to be the greatest obstacles to GDPR compliance.[6]

Enterprise Architects provide access to this information. They act as an interface to numerous stakeholders and can answer almost any question that contributes to GDPR compliance. The basic prerequisite here is that work on the Enterprise Architecture has been well implemented, architectural best practices are applied and modern tools are used.

Of course EAs cannot cover all the requirements of the GDPR; close cooperation between the key managers is therefore indispensable. An initial overview of the various data protection criteria and the interfaces to key managers can be found in the LeanIX GDPR Requirements Catalog (see fig. 2). It will also show you where and how an EA tool can help you with GDPR implementation and when it is advisable to consult the data protection officer and the technology owners.

[6] SearchSecurity: http://www.searchsecurity.de/news/450419077/EU-DSGVO-US-Unternehmen-besser-vorbereitet-als-europaeische-Firmen?

	REQUIREMENT	DESCRIPTION	EA ROLE
1	**Access rights and data portability**	Let users know how, where, for what purpose and by whom their data are processed. Users have the right to transfer their data from one service provider to another.	Can be implemented in Enterprise Architecture Tool (e.g. Data Flow Report)
2	**Right to erasure**	Users have the right to demand their personal data be deleted. Ensure that you can easily trace the storage location of your data in order to erase data.	Can be displayed in the Enterprise Architecture Tool (e.g. Data Object Fact Sheets)
3	**Data protection through technology and as a default approach**	Data protection through technology and as a default approach must be ensured by developing mechanisms for data protection and by introducing monitoring processes.	Can be implemented in the Enterprise Architecture Tool (e.g. querying mechanisms through Surveys)
4	**Geographic range**	Check whether your data processing extends beyond the EU.	Can be displayed in the Enterprise Architecture Tool (e.g. Application Usage Report)
5	**Accountability**	Find out which data are processed where and by whom. Use a data protection program to demonstrate your compliance with the GDPR requirements.	Can be implemented in the Enterprise Architecture Tool (e.g. Data Object Fact Sheets, Interfaces and Application Fact Sheets, Survey)
6	**User consent**	Ensure that you can demonstrate proper consent from users to processing their data.	Contact your data protection officer. EAs can help localize affected applications (e.g. Interface Circle Map, Data Flow Model)
7	**Reporting requirements**	Have you implemented a process to report data protection breaches within 72 hours?	Contact your data protection officer. EAs can help find applications and user groups and provide information (e.g. Visualizer Drill Down Report)
8	**Data protection officer**	Ensure that your company appoints a data protection officer. Contact the data protection officer to define your role in the GDPR process.	Meet with the data protection officer. EAs can answer almost any question that has to be asked in order to ensure proper implementation.

● focus ◍ support

Fig. 2: The GDPR Requirements Catalog

GDPR COMPLIANCE IN FIVE PRACTICAL STEPS WITH EA

1. Contact GDPR stakeholders
2. Identify personal data
3. Detect and assess risks
4. Define checks and implement measures
5. Demonstrate GDPR compliance

1. Contact GDPR stakeholders

Contact other GDPR stakeholders to coordinate your next steps: in many organizations, EAs do not have final responsibility for compliance with legal regulations. This responsibility may lie with your legal department, the chief risk officer, the chief compliance officer, the chief information security officer or the data protection officer. Contact these people in order to coordinate your actions.

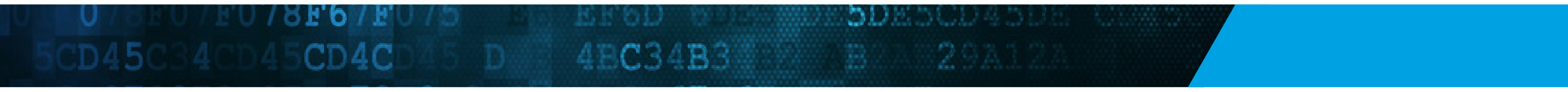
2. Identify personal data

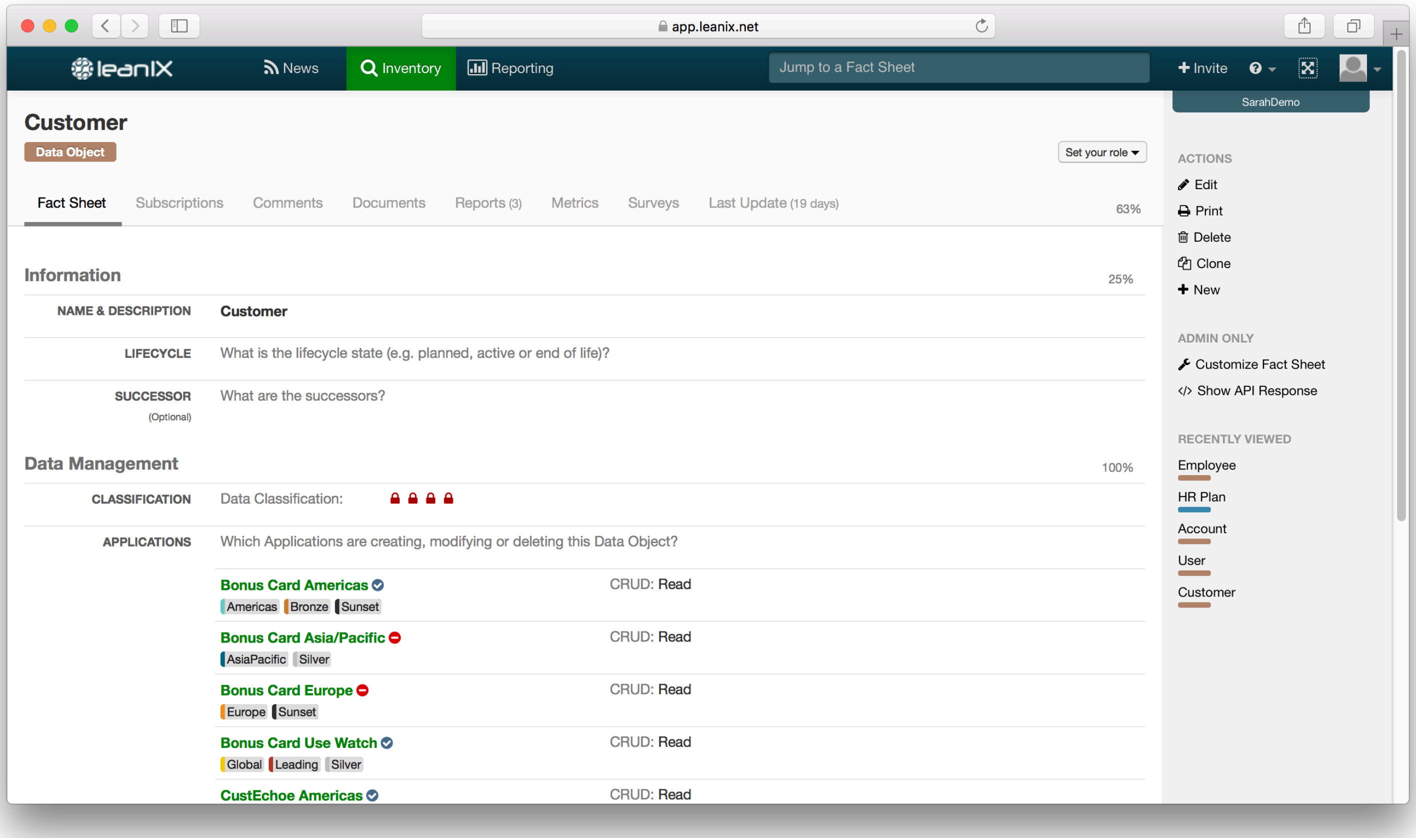
Creating a data inventory is crucial to meeting the requirements of the GDPR documentation. The key to GDPR compliance is having a clear overview of your data - how your company processes it, where it is stored, and how to quickly access it to make key changes. Collecting this information can be a daunting and time-consuming task, and you may not have all of the information that you need.

LeanIX Survey gives you the tools to answer many key GDPR compliance questions, such as: "Who is responsible for the processing of personal data? Which applications use these data? Are they additionally processed and stored outside the EU?" Addressed to the responsible GDPR stakeholders, these can quickly fill out a questionnaire and provide you with the required information through the Survey. Use the "Subscriptions" section in LeanIX (see fig. 4) to identify the responsibilities of individual stakeholders with regard to a specific object.

Subscriptions can also be used in the Filter and the Survey add-on, so you can filter e.g. for all data objects for which a certain user is the data owner. Identify all data that is defined as personal data according to the GDPR. Essentially, any information relating to customer master data and employee data is personal data. Pay particular attention to sensitive data; as the GDPR prohibits their use.

Then assess the data to determine their level of privacy sensitivity, categorizing them as public/unclassified, sensitive, restricted, or confidential. You can use LeanIX tags to add further attributes (e.g. "GDPR restricted") to a data object or application. This will usually already be part of your internal security processes, where you assign attributes such as confidentiality, integrity or availability to data.





app.leanix.net

Customer

Data Object

Set your role

Fact Sheet | Subscriptions | Comments | Documents | Reports (3) | Metrics | Surveys | Last Update (19 days) | 63%

Information 25%

NAME & DESCRIPTION	Customer
LIFECYCLE	What is the lifecycle state (e.g. planned, active or end of life)?
SUCCESSOR (Optional)	What are the successors?

Data Management 100%

CLASSIFICATION	Data Classification: 🔒🔒🔒🔒
APPLICATIONS	Which Applications are creating, modifying or deleting this Data Object?

Bonus Card Americas ✓ Americas Bronze Sunset	CRUD: Read
Bonus Card Asia/Pacific ⊖ AsiaPacific Silver	CRUD: Read
Bonus Card Europe ⊖ Europe Sunset	CRUD: Read
Bonus Card Use Watch ✓ Global Leading Silver	CRUD: Read
CustEchoe Americas ✓	CRUD: Read

ACTIONS
- Edit
- Print
- Delete
- Clone
- New

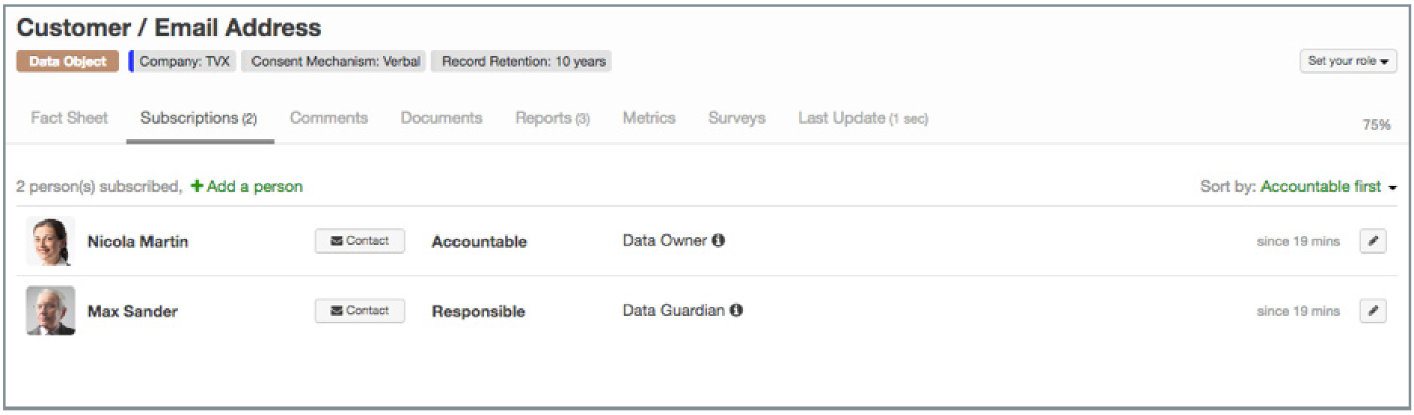
ADMIN ONLY
- Customize Fact Sheet
- Show API Response

RECENTLY VIEWED
- Employee
- HR Plan
- Account
- User
- Customer

Fig.3 Identifying data objects and categorizing them by privacy sensitivity in LeanIX

Finally, describe the purpose for which certain data was collected (e.g. payroll accounting, customer competition) and ensure that you have (or get) the consent of the data subjects. You can enter this information in the "Description" field of the data object.

We recommend using reports such as the Heat Map in this phase. It will help you localize any applications that process sensitive data and identify business capabilities that use the applications in question (see fig. 5).



Customer / Email Address

Data Object | Company: TVX | Consent Mechanism: Verbal | Record Retention: 10 years

Set your role

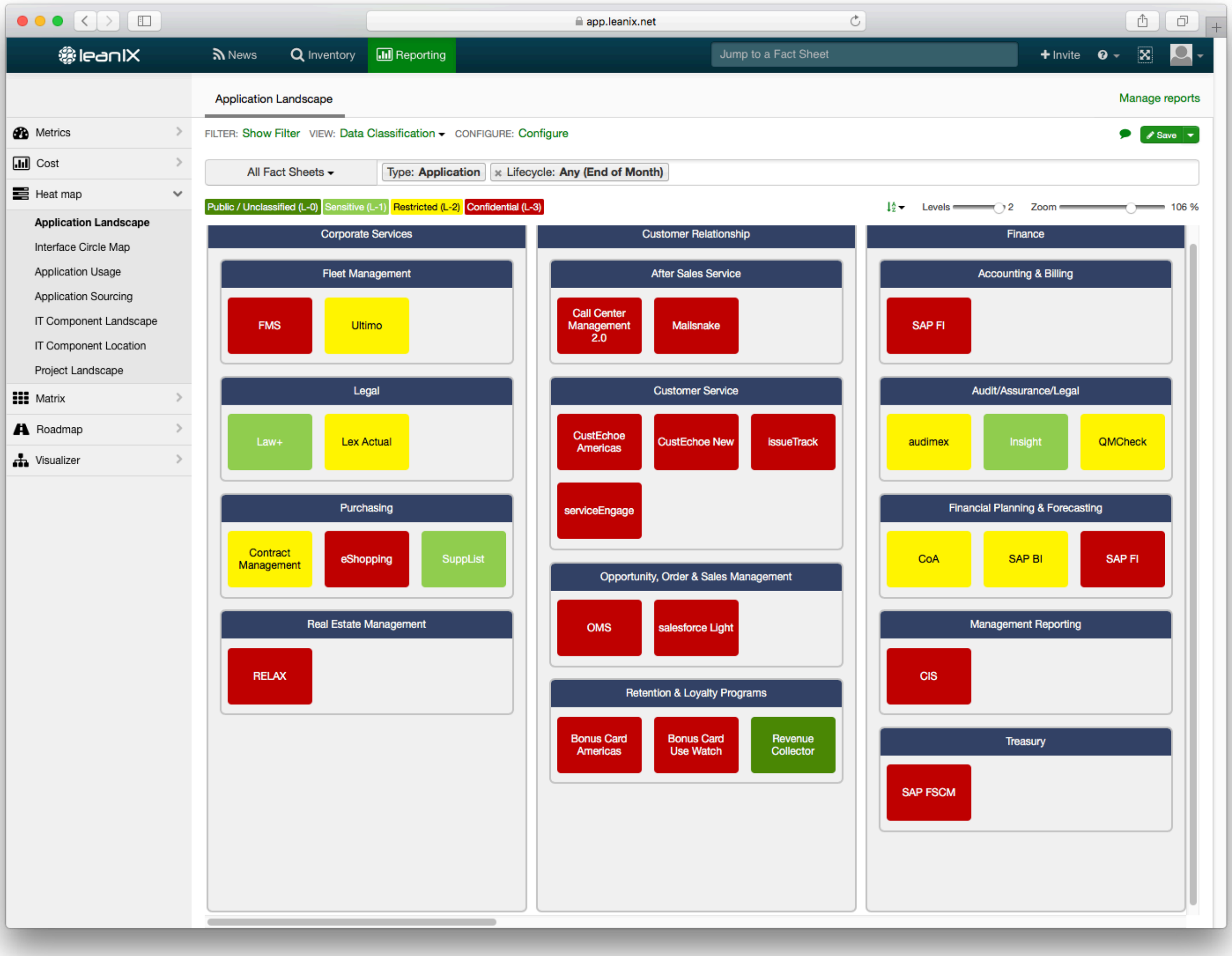
Fact Sheet | Subscriptions (2) | Comments | Documents | Reports (3) | Metrics | Surveys | Last Update (1 sec) | 75%

2 person(s) subscribed, + Add a person

Sort by: Accountable first

Nicola Martin	Contact	Accountable	Data Owner ℹ	since 19 mins
Max Sander	Contact	Responsible	Data Guardian ℹ	since 19 mins

Fig.4 Identifying responsibilities and ownership of data objects in LeanIX



Application Landscape

Interface Circle Map

Application Usage

Application Sourcing

IT Component Landscape

IT Component Location

Project Landscape

Application Landscape

FILTER: Show Filter VIEW: Data Classification CONFIGURE: Configure

All Fact Sheets | Type: Application | Lifecycle: Any (End of Month)

Public / Unclassified (L-0) | Sensitive (L-1) | Restricted (L-2) | Confidential (L-3)

Corporate Services
- Fleet Management: FMS, Ultimo
- Legal: Law+, Lex Actual
- Purchasing: Contract Management, eShopping, SuppList
- Real Estate Management: RELAX

Customer Relationship
- After Sales Service: Call Center Management 2.0, Mailsnake
- Customer Service: CustEchoe Americas, CustEchoe New, IssueTrack, serviceEngage
- Opportunity, Order & Sales Management: OMS, salesforce Light
- Retention & Loyalty Programs: Bonus Card Americas, Bonus Card Use Watch, Revenue Collector

Finance
- Accounting & Billing: SAP FI
- Audit/Assurance/Legal: audimex, Insight, QMCheck
- Financial Planning & Forecasting: CoA, SAP BI, SAP FI
- Management Reporting: CIS
- Treasury: SAP FSCM

Fig. 5: Classifying data with Heat Maps in LeanIX

3. Detect and assess risks

Around 76% of German businesses state that due to the complexity of modern IT services, they do not always know where their customer data is located. Imagine a consumer wants to make use of her "right to be forgotten". In order to delete her data, you have to know where they are stored. An EA tool like LeanIX is the basis for effectively implementing these processes.

Automated visualizations such as the Data Flow Model show which data objects are used by which applications and which business capabilities in turn depend on them. The data flow is generated automatically and can be expanded by adding details such as the IT components and user groups of certain applications. Labels next to the interfaces display their attributes, such as interface technology, data objects and frequency.

Then assess your application landscape for risk. The level of risk can be determined through a range of different parameters, in particular however with regard to the business impact, application dependencies, criticality levels, failure scenarios and previous incidents.

Visualizations such as the above-described Heat Map can provide information on business-critical consequences for your company in the event of an application failure or hacking attack (see fig. 7). Risk Dependency Maps and Interface Circle Maps visualize the various dependencies between multiple applications. The more dependencies an application has, the higher the level of risk in the event of a failure (see fig. 8–9). You can additionally use a Survey when querying information on possible failure scenarios and incidents in the past in order to assess the risk level.

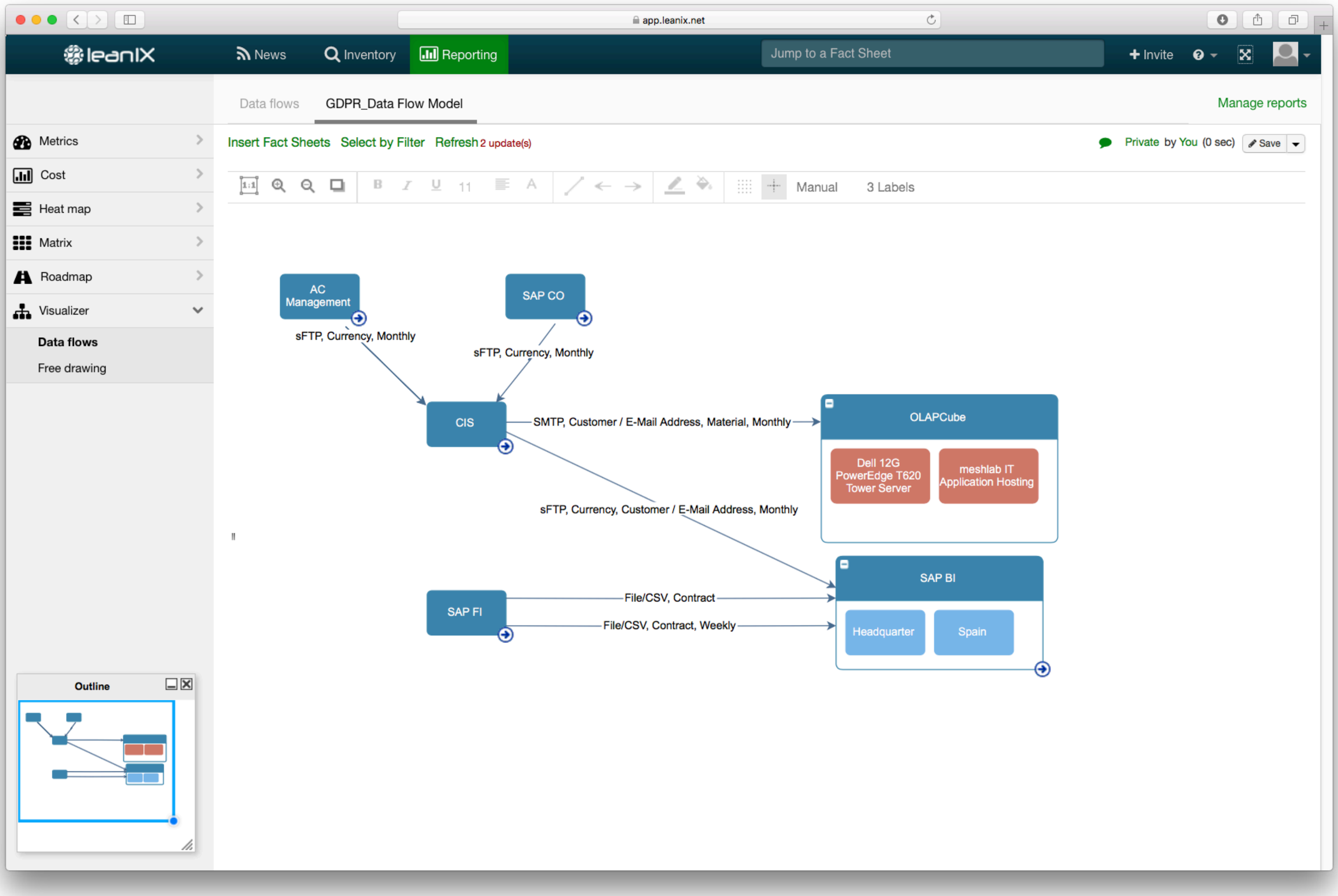
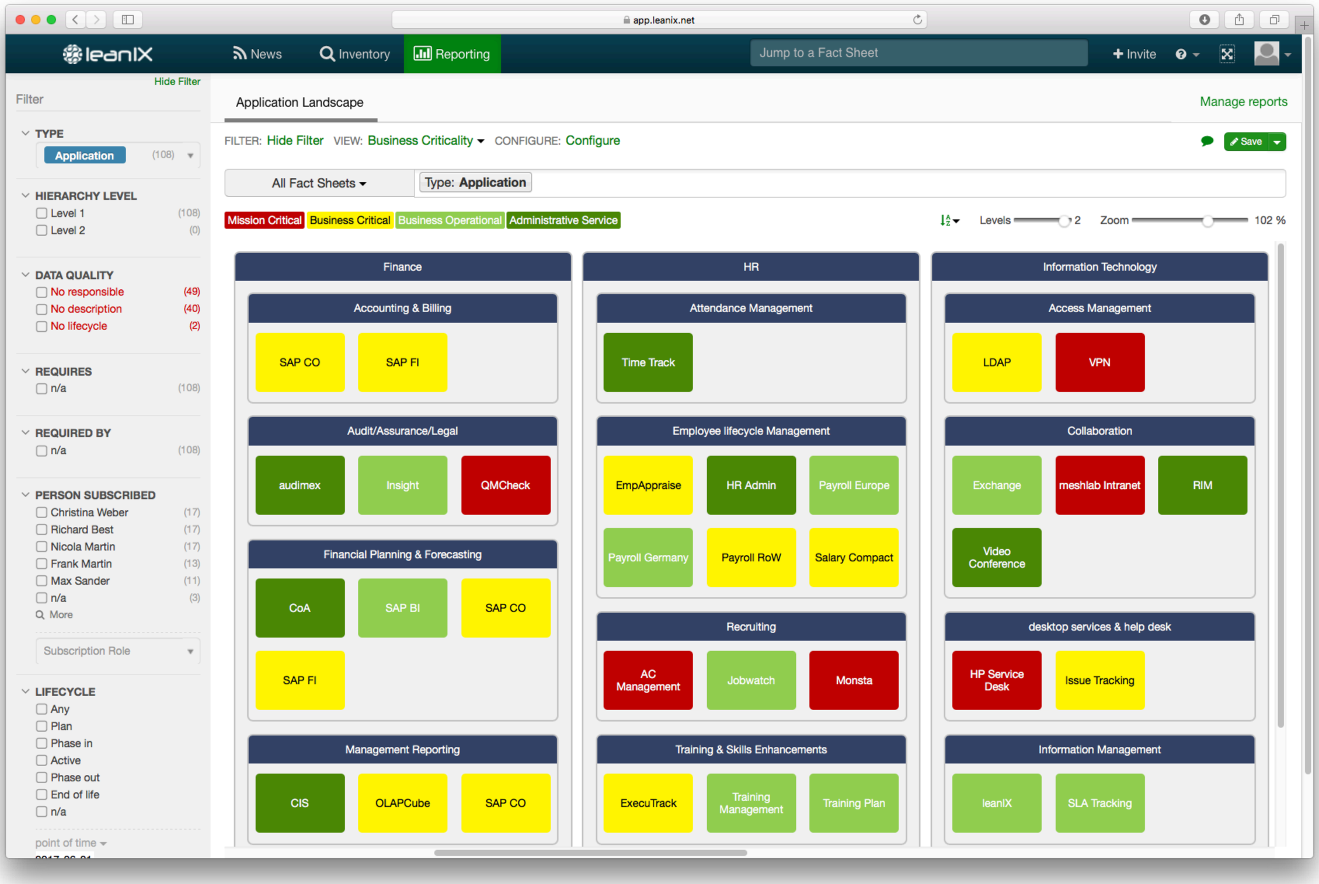


Fig. 6: Data Flow Model in LeanIX



Hide Filter

Filter

TYPE
Application (108)

HIERARCHY LEVEL
- □ Level 1 (108)
- □ Level 2 (0)

DATA QUALITY
- □ No responsible (49)
- □ No description (40)
- □ No lifecycle (2)

REQUIRES
- □ n/a (108)

REQUIRED BY
- □ n/a (108)

PERSON SUBSCRIBED
- □ Christina Weber (17)
- □ Richard Best (17)
- □ Nicola Martin (17)
- □ Frank Martin (13)
- □ Max Sander (11)
- □ n/a (3)

More

Subscription Role

LIFECYCLE
- □ Any
- □ Plan
- □ Phase in
- □ Active
- □ Phase out
- □ End of life
- □ n/a

point of time

Application Landscape

Manage reports

FILTER: Hide Filter VIEW: Business Criticality CONFIGURE: Configure

Save

All Fact Sheets Type: Application

Mission Critical | Business Critical | Business Operational | Administrative Service

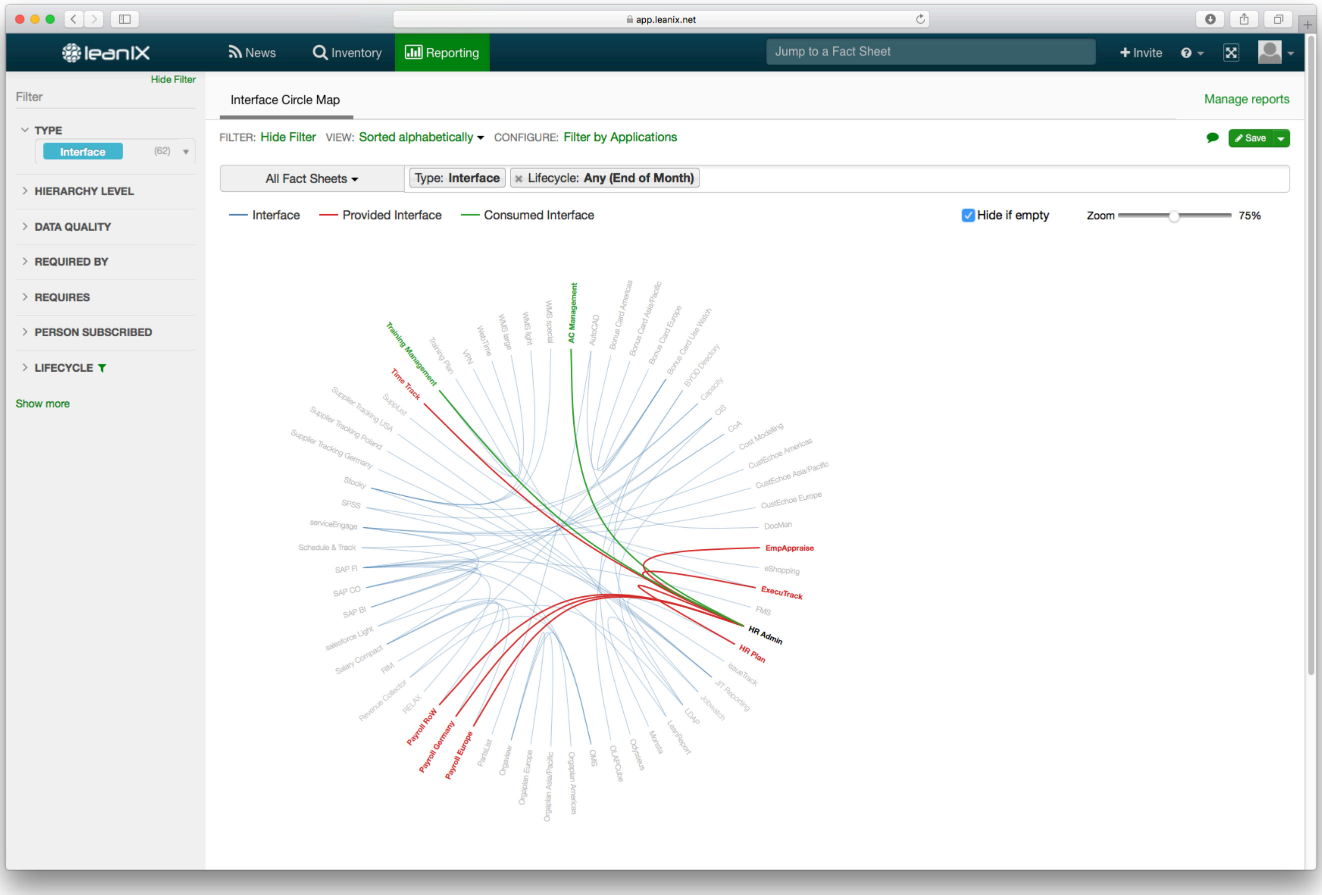
Levels 2 Zoom 102 %

Finance
- Accounting & Billing: SAP CO, SAP FI
- Audit/Assurance/Legal: audimex, Insight, QMCheck
- Financial Planning & Forecasting: CoA, SAP BI, SAP CO, SAP FI
- Management Reporting: CIS, OLAPCube, SAP CO

HR
- Attendance Management: Time Track
- Employee lifecycle Management: EmpAppraise, HR Admin, Payroll Europe, Payroll Germany, Payroll RoW, Salary Compact
- Recruiting: AC Management, Jobwatch, Monsta
- Training & Skills Enhancements: ExecuTrack, Training Management, Training Plan

Information Technology
- Access Management: LDAP, VPN
- Collaboration: Exchange, meshlab Intranet, RIM, Video Conference
- desktop services & help desk: HP Service Desk, Issue Tracking
- Information Management: leanIX, SLA Tracking

Fig. 7: Heat Map of business impact in LeanIX



Hide Filter

Filter

TYPE
Interface (62)

HIERARCHY LEVEL

DATA QUALITY

REQUIRED BY

REQUIRES

PERSON SUBSCRIBED

LIFECYCLE

Show more

Interface Circle Map

Manage reports

FILTER: Hide Filter VIEW: Sorted alphabetically CONFIGURE: Filter by Applications

Save

All Fact Sheets Type: Interface × Lifecycle: Any (End of Month)

Interface | Provided Interface | Consumed Interface

☑ Hide if empty Zoom 75%

Fig. 8: Identifying dependencies with the Interface Circle Map in LeanIX

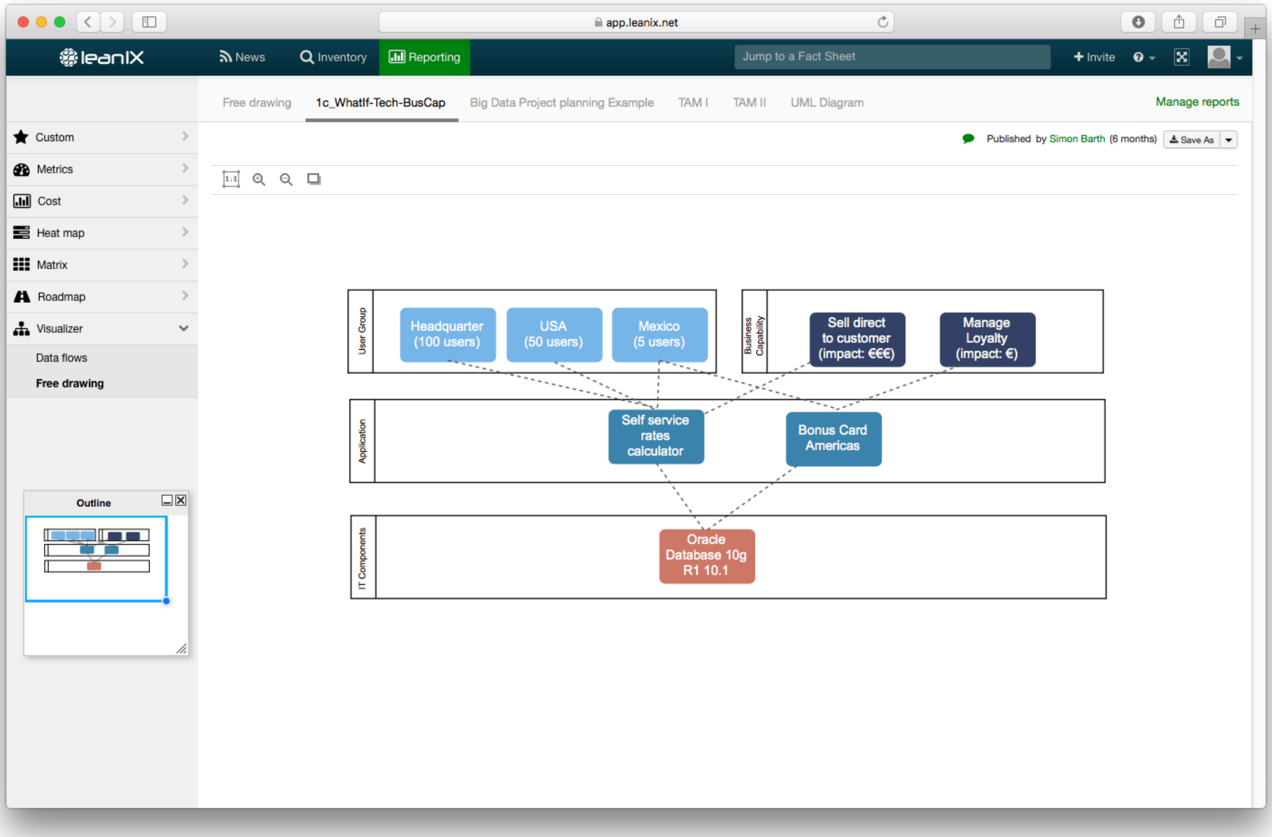
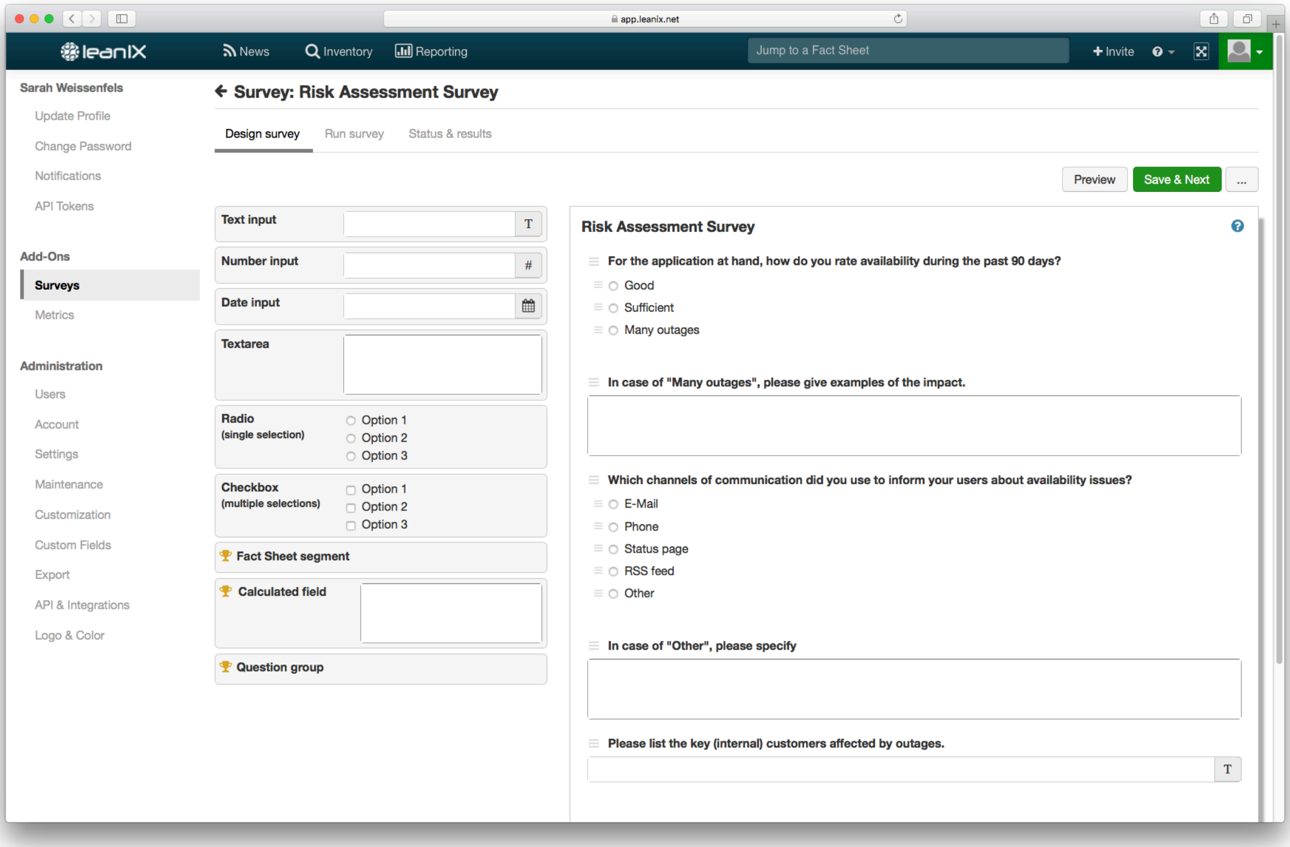


Fig. 9: Risk Dependency Map in LeanIX



Survey: Risk Assessment Survey

Risk Assessment Survey

For the application at hand, how do you rate availability during the past 90 days?

○ Good
○ Sufficient
○ Many outages

In case of "Many outages", please give examples of the impact.

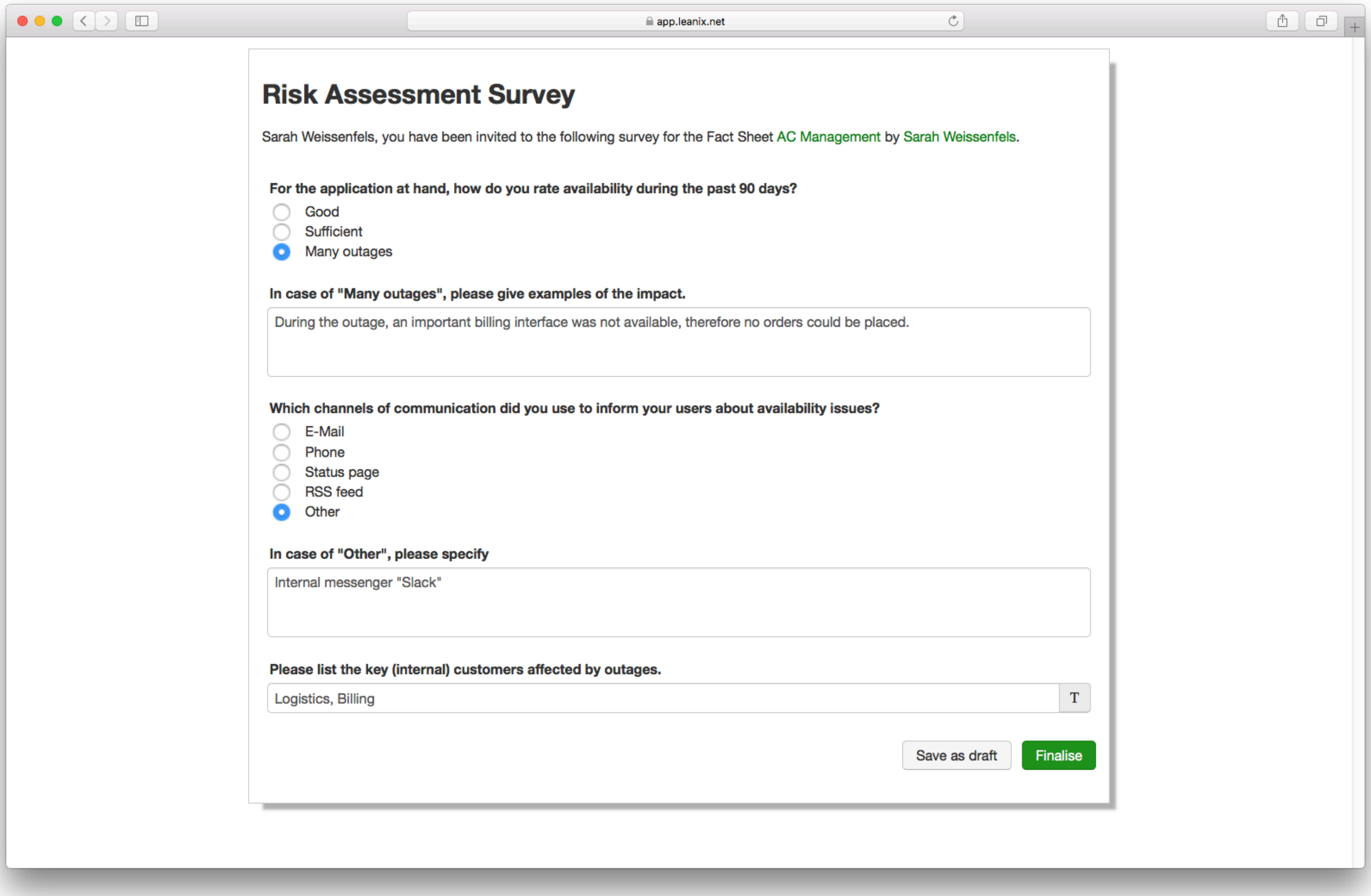
Which channels of communication did you use to inform your users about availability issues?

○ E-Mail
○ Phone
○ Status page
○ RSS feed
○ Other

In case of "Other", please specify

Please list the key (internal) customers affected by outages.

Fig.10: Risk Survey in LeanIX 1/2



Risk Assessment Survey

Sarah Weissenfels, you have been invited to the following survey for the Fact Sheet AC Management by Sarah Weissenfels.

For the application at hand, how do you rate availability during the past 90 days?

○ Good
○ Sufficient
● Many outages

In case of "Many outages", please give examples of the impact.

During the outage, an important billing interface was not available, therefore no orders could be placed.

Which channels of communication did you use to inform your users about availability issues?

○ E-Mail
○ Phone
○ Status page
○ RSS feed
● Other

In case of "Other", please specify

Internal messenger "Slack"

Please list the key (internal) customers affected by outages.

Logistics, Billing

Fig.10: Risk Survey in LeanIX 2/2

We recommend starting with areas that have a high risk factor and process sensitive data. Answer questions such as: Where could potential vulnerabilities in the business and IT landscape lie? What are frequent threats that could exploit these vulnerabilities? What are the possible consequences?

For example, think of an application that is deeply embedded in the IT landscape via multiple interfaces. If it fails, the effects can be severe. Imagine a CRM system that plays a major role for customer data and has interfaces to Microsoft Exchange, mailing tools, help desk tools, content management systems and much more. Its high level of connectivity means the potential effects on other applications and processes are multiplied. Heat Maps, Interface Circle Maps, and Risk Dependency Maps help you gain an overview of your company's risk portfolio and thus serve important decision-makers as a first basis for risk management and control.

4. Define checks and implement measures

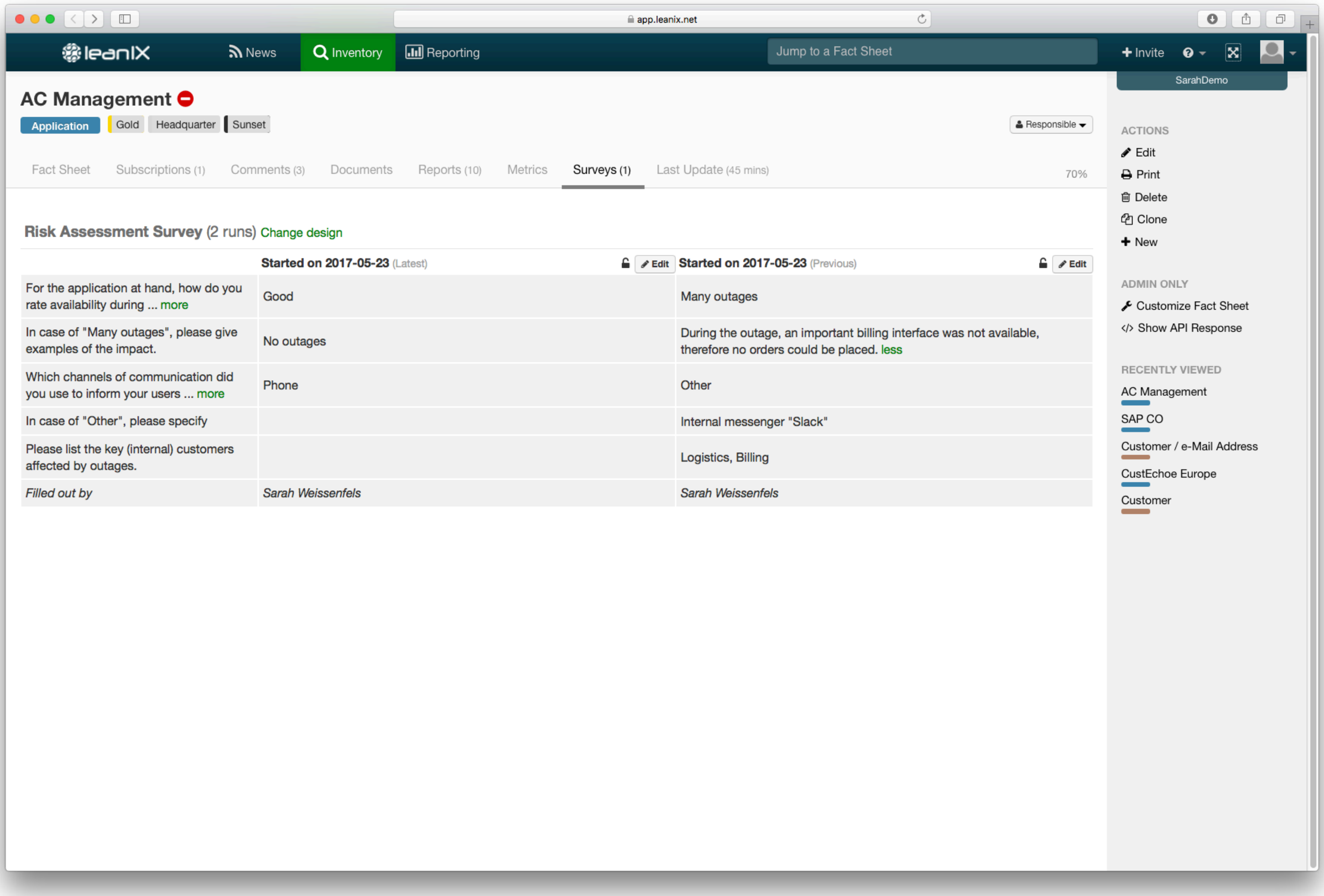
Once you have correctly assessed the technology risks, you need to implement concrete security checks and preventative measures. The IT security checks in ISO 27001 can serve as a guideline here. Introduce important measures as soon as possible in order to implement the data protection by technology approach (e.g. pseudonymizing personal data); this will save you time and money when upgrading. Always ask yourself:

How well does your application portfolio meet security standards? How are your security standards developing over time?

LeanIX Survey feature provides the initial answers as a starting point for defining useful security checks and appropriate measures. Imagine a content management system that collects customer data that in turn are transfered to mailing tools and CRM systems via a range of interfaces. Survey allows you to query and identify deficits in your IT landscape, e.g. if your company currently has no demonstrable consent from the addressees because the application owner has not implemented a double opt-in process. The responsible owner can provide possible recommendations for preventative measures via the comment field in the Survey feature.

Further vulnerabilities, such as the recording of non-relevant or duplicate data, can also be queried via a Survey. If your company is for example collecting entrant data for an online competition (e.g. name, address and date of birth), only the first two items are required to determine the winner, whereas the date of birth is not. You must therefore point out that submitting these data is voluntary and indicate why you are requesting them (rule of data minimization). LeanIX will help you uncover vulnerabilities and systematically follow up on their correction.

Then transfer the measures you have defined in your organization, your processes and systems into projects. The previously described Survey can be used repeatedly over a longer period of time to monitor the checking process and document the development of measures. Comparing the results will assist you in the GDPR implementation process.



AC Management

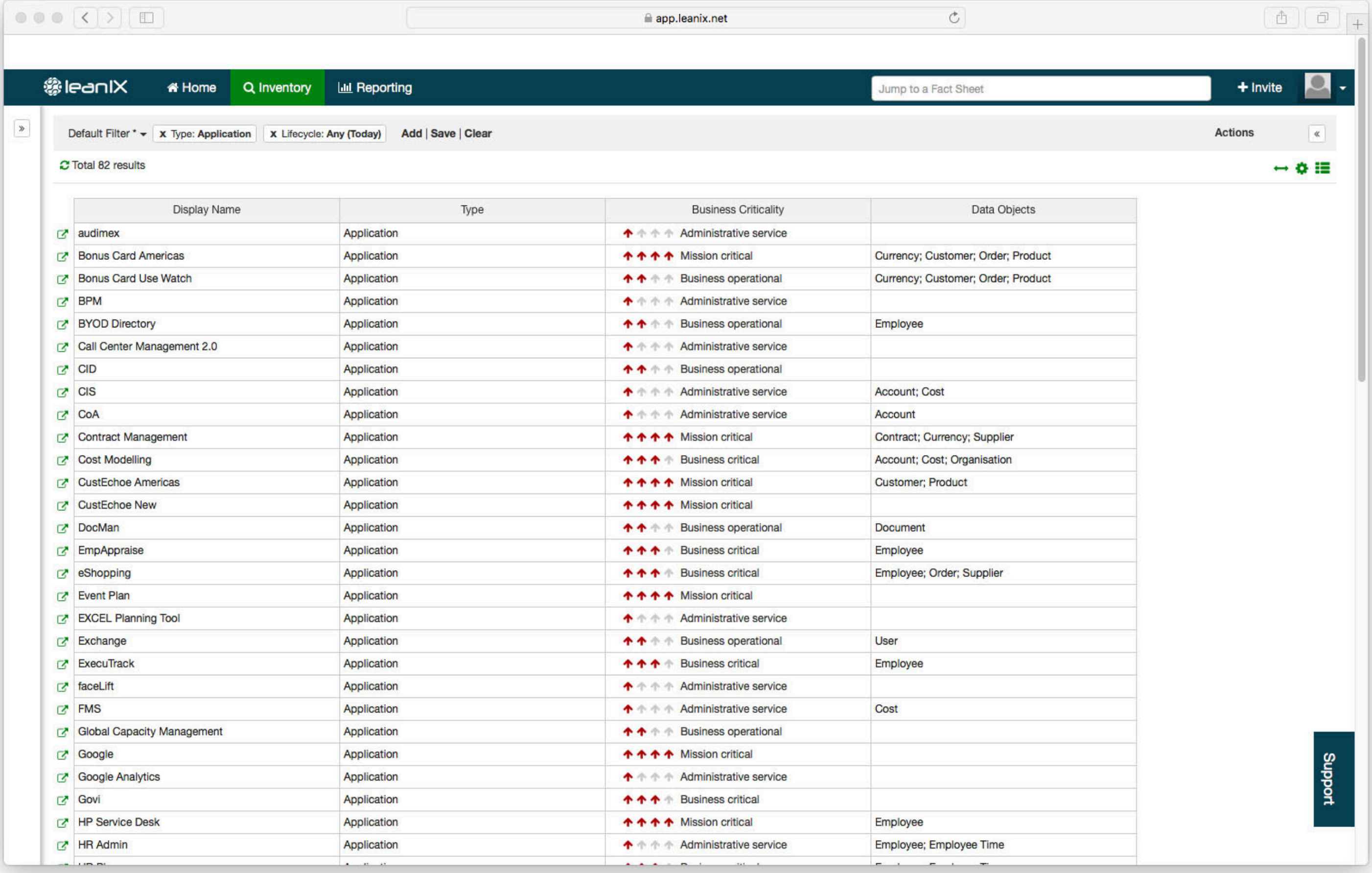
Risk Assessment Survey (2 runs) Change design

	Started on 2017-05-23 (Latest) Edit	Started on 2017-05-23 (Previous) Edit
For the application at hand, how do you rate availability during ... more	Good	Many outages
In case of "Many outages", please give examples of the impact.	No outages	During the outage, an important billing interface was not available, therefore no orders could be placed. less
Which channels of communication did you use to inform your users ... more	Phone	Other
In case of "Other", please specify		Internal messenger "Slack"
Please list the key (internal) customers affected by outages.		Logistics, Billing
Filled out by	*Sarah Weissenfels*	*Sarah Weissenfels*

Fig. 11: Survey query over a specific period in LeanIX

5. Demonstrate GDPR compliance

Demonstrate your compliance with GDPR guidelines by showing how you process personal data, how you handle risks and what measures for damage limitation you have implemented. The latter is especially relevant when you conduct a DPIA, which the GDPR requires for every implementation of a new system that uses personal data. Use the LeanIX Inventory View function and present your GDPR compliance by providing a quick and clear overview in table form of all applications, interfaces, data objects and technologies.



x Type: Application

x Lifecycle: Any (Today)

Total 82 results

Display Name	Type	Business Criticality	Data Objects
audimex	Application	Administrative service	
Bonus Card Americas	Application	Mission critical	Currency; Customer; Order; Product
Bonus Card Use Watch	Application	Business operational	Currency; Customer; Order; Product
BPM	Application	Administrative service	
BYOD Directory	Application	Business operational	Employee
Call Center Management 2.0	Application	Administrative service	
CID	Application	Business operational	
CIS	Application	Administrative service	Account; Cost
CoA	Application	Administrative service	Account
Contract Management	Application	Mission critical	Contract; Currency; Supplier
Cost Modelling	Application	Business critical	Account; Cost; Organisation
CustEchoe Americas	Application	Mission critical	Customer; Product
CustEchoe New	Application	Mission critical	
DocMan	Application	Business operational	Document
EmpAppraise	Application	Business critical	Employee
eShopping	Application	Business critical	Employee; Order; Supplier
Event Plan	Application	Mission critical	
EXCEL Planning Tool	Application	Administrative service	
Exchange	Application	Business operational	User
ExecuTrack	Application	Business critical	Employee
faceLift	Application	Administrative service	
FMS	Application	Administrative service	Cost
Global Capacity Management	Application	Business operational	
Google	Application	Mission critical	
Google Analytics	Application	Administrative service	
Govi	Application	Business critical	
HP Service Desk	Application	Mission critical	Employee
HR Admin	Application	Administrative service	Employee; Employee Time

Fig. 12: Inventory View in LeanIX

Regularly reviewing GDPR compliance and demonstrating data currency is easy if you have a current data basis on your IT landscape. LeanIX helps you achieve this transparency and offers many ways of ensuring that your data are always up to date. You can for example access your Surveys, where you have documented the entire progress of your GDPR implementation. Data quality workflows help responsible managers ensure their data are up to date at regular intervals. And the collaborative elements of LeanIX enable all GDPR stakeholders to easily work together on a single platform.

SUMMARY

The new EU directive is causing concern in many companies. Business owners are hesitant to implement the GDPR and face the major challenge of becoming GDPR compliant by May 25, 2018. According to a recent survey, around 50% of all organizations will not be able to meet the regulatory requirements on time, leading them susceptible high fines and penalties.

Preparing for the GDPR requires precise information on which data your company stores and processes. Having accessible and adjustable data is the key to GDPR compliance.

LeanIX software gives EAs the tools to master data protection obstacles and outlines a 5 step model to successful GDPR compliance. The LeanIX GDPR Requirements Catalog helps you gain an initial overview of your data, where and how it is stored and sets the framework to answer pertinent questions which can potentially save your company millions in fines.

May 2018 is quickly approaching. Is your organization ready for GDPR?

Copyright

This document is current at the time of its initial publication. LeanIX GmbH reserves the right to alter it at any time.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED AS IS, WITH NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLICIT.

Document version 1.1

About LeanIX

LeanIX offers a Software-as-a-Service (SaaS) for Enterprise Architecture (EA), which enables organizations to take faster, data-driven decisions for their IT landscape. More than 80 leading brands such as adidas, DHL, Merck, Vodafone, and Zalando use the innovative solution worldwide. Users of LeanIX gain insights on how to organize and leverage their IT landscape to increase competitiveness and enable innovation going forward. LeanIX addresses the frequent problem that the required information about the IT landscape is missing, outdated, or difficult to analyze. Use cases include application rationalization, technology risk management, and the shift from monolithic architectures to microservices. LeanIX was founded in 2012 by Jörg Beyer and André Christ. The company's headquarter is in Bonn, Germany, with offices in Boston, Massachusetts, and Houston, Texas. A wide network of partners provides support in America, Europe, and Australia.

[7] Gartner: https://www.gartner.com/doc/reprints?id=1-3V903Y9&ct=170309&st=sg

LeanIX GmbH
Bonn
Germany

Tel: +49 (0) 228 2862992-0
Email: info@leanix.net
www.leanix.net