LUT University
School of Engineering Science
Degree Program in Computer Science

Master's Thesis

Jari Kauppila

IMPLEMENTING GDPR REQUIREMENTS IN A SIEBEL BASED IT ORGANIZATION

Examiners: Professor Jari Porras
Assistant Professor Antti Knutas

Supervisor: Professor Jari Porras

ABSTRACT

LUT University
School of Engineering Science
Degree Program in Computer Science
Jari Kauppila

Implementing GDPR requirements in a Siebel based IT organization
Master's Thesis
55 pages, 9 figures
Examiners: Professor Jari Porras
Assistant Professor Antti Knutas
Keywords: GDPR, private data, personal data, data protection

The European Union has passed a new regulation in response to a growing number of threats to privacy: the General Data Protection Regulation. The goal of this thesis is to make the IT systems of the target company ready for GDPR. The focus will be on the Siebel system by Oracle, which will be the most important system as far as contact data is concerned. GDPR allows people to get a copy of all of their personal data or get it modified, deleted or locked from modifications. It also requires controllers (those who have the data) to notify of breaches within 72 hours and to have a comprehensive plan on keeping data secure. To make it easier to respond to data protection requests Konecranes decided to make Siebel the contact data master so that if contact data is changed there, it is changed everywhere. However, such a large project did not get ready in time so a data protection support ticket process was set up where a ticket will be divided into sub-tickets, each of which are sent to a system administrator. For Siebel contact data, new fields were added for marketing prohibition and locking the data. For new system development a Data Protection Impact Assessment process was defined that must be performed at the design phase of the software development life cycle.

TIIVISTELMÄ

LUT University
School of Engineering Science
Tietotekniikan koulutusohjelma
Jari Kauppila
GDPR-vaatimusten toteuttaminen Siebel-pohjaisessa IT-organisaatiossa
Diplomityö
2018

55 sivua, 9 kuvaa
Työn tarkastajat: Professori Jari Porras
Apulaisprofessori Antti Knutas
Hakusanat: GDPR, yksityinen data, henkilökohtainen data, datan suojaus

Euroopan unioni hyväksyi uuden ohjesäännön vastauksena yksityisyyden uhkiin Internetissä: GDPR (General Data Protection Regulation). Työn tavoitteena on saada kohdeyrityksen IT-järjestelmät GDPR-valmiiksi. Työssä keskitytään Oraclen kehittämään Siebel-järjestelmään, mikä on kontaktidatan kannalta tärkein järjestelmä. GDPR antaa ihmisille valtuuden hankkia kopio henkilökohtaisesta datastaan tai saada se poistetuksi, muokatuksi tai lukituksi muokkauksilta. Se vaatii myös datan omistajia kertomaan murroista 72 tunnin sisällä ja laatimaan suunnitelman miten henkilökohtainen data pidetään turvassa. Helpottaakseen kontaktidatan käsittelyä ja GDPR-pyyntöjen toteuttamista Konecranes päätti tehdä Siebel-järjestelmästä keskuksen kontaktidatalle niin, että jos data muuttuu siellä, se muuttuu kaikissa järjestelmissä. Näin iso projekti ei kuitenkaan valmistunut heti, joten väliaikaisratkaisuna GDPR-pyynnöille on toteutettu erillinen prosessi, jossa tiketti jaetaan useisiin pienempiin tiketteihin, jotka annetaan eri järjestelmien ylläpitäjille. Siebelin kontaktidatalle lisättiin markkinointikielto- ja datalukkokentät. Uusien järjestelmien kehitysprosessia muutettiin niin, että suunnittelu-vaiheessa suoritetaan datansuojauksen vaikutusarviointi.

ACKNOWLEDGEMENT

I have been a student in Lappeenranta University of Technology for eight years. It has taken me a long time to get to this point, and making this thesis has been the most difficult part of it. But now I'm ready to finish my master's degree.

I would like to thank my manager Tuomas Pyyhtiä for being there to assist me at work and for telling me along with Mikko Heikkilä about this project that I ended up making my master’s thesis about. As of this writing, you're leaving Konecranes for Kone. I wish you good luck with the transition to a new work place.

Extra special thanks go to my brother who tipped me off about the open spot at Konecranes in the first place. More thanks go to my parents who kept cheering me on even though making this thesis took me a longer time than I originally estimated.

Jari Kauppila

SISÄLLYSLUETTELO

SYMBOLS AND ABBREVIATIONS

EU	European Union
GDPR	General Data Protection Regulation
PME	Preventive maintenance engine
IT	Information technology
CRM	Customer relationship management
VPN	Virtual private network
DPIA	Data protection impact assessment
MDM	Master data maintenance
FS	Field service
FSSC	Financial shared services center
GCM	Global Company Master
EMEA	Europe, Middle East and Africa
KC	Konecranes

1 INTRODUCTION

The European Union (EU) introduced a new regulation called the General Data Protection Regulation in April 2016. Its purpose is to regulate large multi-national tech corporations whose business model is to offer services for free but with targeted advertising. Targeted advertising requires companies to collect as much personal data of its users as they can so that they can properly guess what kind of products the user would want, maximizing the clicks that their advertising gets. This can be achieved either through tracking the user's online use or by having the user submit all that information (common in social media services). The goal of GDPR is to allow citizens of the EU to have more control over their private data and to improve the privacy of the citizens' sensitive data.

The stakes are high because failure to comply with GDPR requirements comes with extremely high penalties. In the worst case scenario the fine for breaking the law will be 4% of the gross domestic product of the company.

Although the regulation appears to be aimed at customer-facing companies that collect large amounts of data, the regulation applies to everyone. The case company of this work – Konecranes – is operating in the business-to-business market so it is not in a position where it holds private information of large amounts of customers. However, it does have lots of contact data for other businesses and some of their workers, which is considered private data by the regulation. Therefore GDPR will create a responsibility for protecting this data.

1.1 The problem

The purpose of this project is to make Konecranes' IT business compliant with GDPR. The company has quite many IT systems in use, so much of the personal data is scattered around and difficult to get. A process for completing GDPR requests must be established and the company's IT infrastructure needs to be set up in a way to make it as easy as possible to comply with data protection regulations.

The thesis will put extra focus on Oracle's Siebel CRM (customer relationship management) system, which is the main CRM system used by Konecranes. Siebel is one of the most important systems in the company as Konecranes continues its project to harmonize processes and get all different regional branches to use Siebel. The general process of how GDPR requests are handled will also be discussed, but making Siebel compliant is the primary focus.

1.2 Structure of the thesis

The second chapter will introduce Konecranes, which is the case company for this thesis. It will also introduce the IT sector of the company which this thesis has been done for.

The third chapter of the work goes through some previous literature that has been written about GDPR and the general concept of privacy. It will also go through some recent events (since 2014) that may have inspired the creation of the regulation. The fourth chapter will be an introduction to the GDPR regulation itself, which is what Konecranes will be trying to adhere to.

The fifth chapter will detail what kind of measures Konecranes has taken as a company to ensure GDPR compliance. These are the company-wide initiatives that have been taken, not limited to Siebel only.

The sixth chapter introduces Siebel, the main focus of this thesis. It will go through how Siebel data is organized and how Konecranes has divided it between Field Service and CRM (customer relationship management). With some basic Siebel knowledge, the seventh chapter will then go through what changes have been made to make Siebel GDPR compliant.

The eighth chapter will go through the new process that will be gone through if a data protection request is received. Data protection requests are one of the biggest new rights that GDPR has given so it is important to go through the process thoroughly.

Finally, all of the above will be summarized and there will be a couple of thoughts on how the company will proceed in the future and how GDPR will affect operations going forward.

2 THE CASE COMPANY: KONECRANES

This chapter will introduce the case company that this thesis has been created for.

Konecranes is a Finnish industrial company whose headquarters are located in Hyvinkää. It specializes in lifting equipment, offering both new equipment and services to existing equipment. Its customers include shipyards, ports, terminals and manufacturing and process industries.

Konecranes' business is organized into three business areas: Service, Industrial Equipment and Port Solutions. Service provides maintenance to cranes and hoists, including those bought from other companies. Industrial Equipment offers lifting solutions for industrial purposes, such as cranes and hoists. Port Solutions offers equipment for shipyards and transportation, such as mobile harbor cranes, lift trucks and container handling equipment.

2.1 Lifecycle Care in Real Time

The primary approach for service is Lifecycle Care in Real Time, which provides a complete maintenance program for the lifecycle of the customer's product to maximize the value of the product and minimize downtime. A quick overview graphic of Lifecycle Care is provided in Figure 1 as seen on Konecranes' web site. [1]

The process starts with purchasing new equipment. A Lifecycle Care contract includes periodic inspections and preventive maintenance to identify risks before anything happens. If issues arise anyway, corrective maintenance is included so the issue can be fixed. Consultation services allow Konecranes employees to train employees to get the most out of the purchased product and inspect components for non-critical issues that may slow down work. Modernization services will prolong the life of the equipment and possibly improve its performance. The cycle will begin anew when the equipment gets replaced, starting the process again for new equipment.

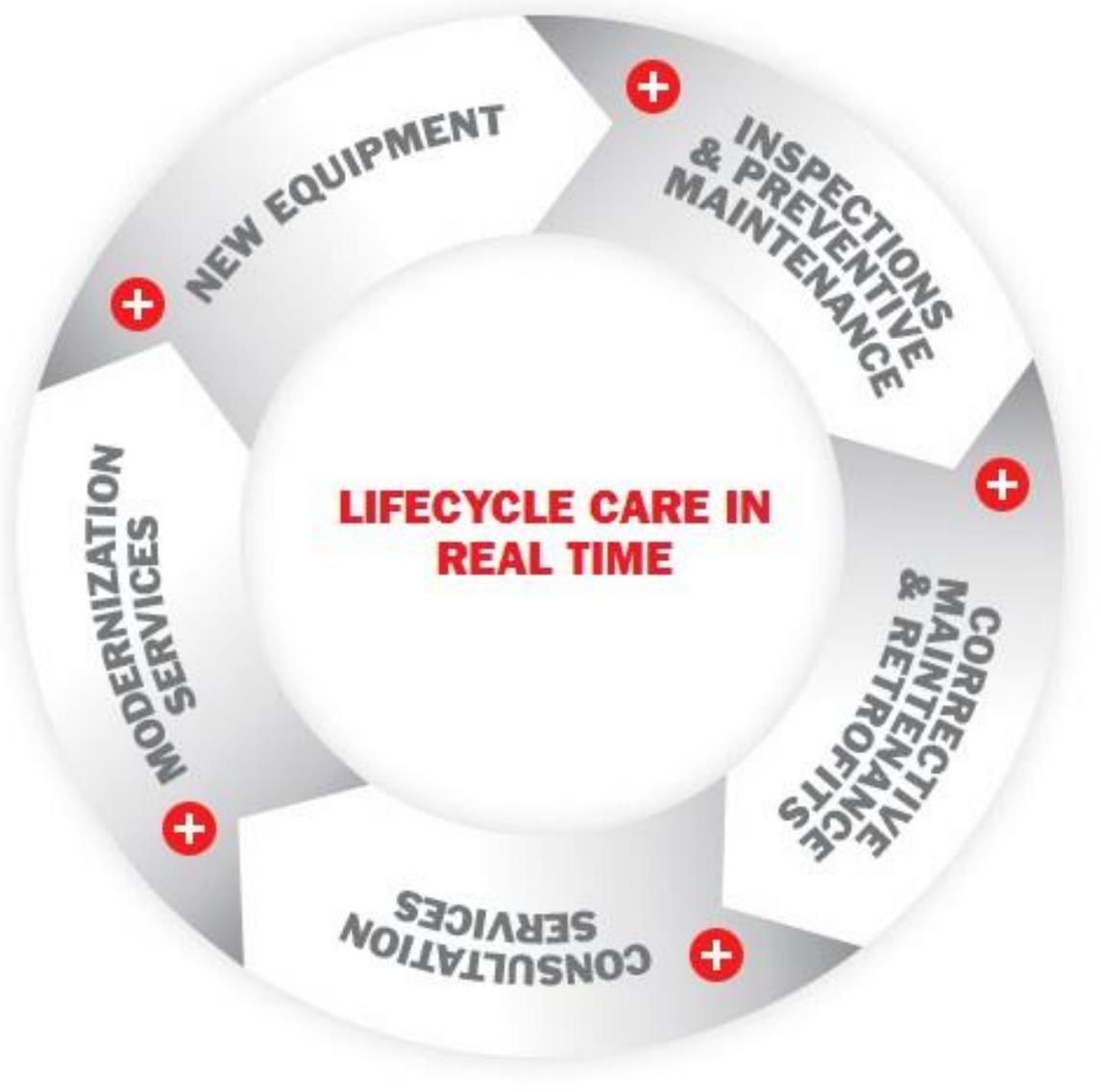

Figure 1: Lifecycle Care in Real Time process as advertised by Konecranes

2.2 IT

Konecranes IT is an organization within Konecranes that provides IT services to Konecranes customers and employees.

The long term goal for Konecranes IT is to create a smarter service to make customers' operations even smarter and more productive with less downtime. The vision is to receive real time information of the performance of millions of lifting devices, allowing the

company to offer services when needed before the customer may even be aware that their equipment needs service.

"We develop information technology to make Konecranes the technology leader in lifting businesses." – Konecranes IT mission

In addition to smart systems such as remote crane operation, Konecranes uses IT for customer relationship management and employee data handling. The primary customer relationship management system in use is Siebel Field Service, which is currently owned and maintained by Oracle. Siebel Field Service features a Preventive Maintenance Engine (PME) that will automatically generate work for service technicians, helping to achieve the goals of Lifecycle Care in Real Time. Both sales persons and service technicians use Siebel in their daily work.

Siebel is a system that keeps records of all companies that Konecranes has dealt with (both customers and part suppliers) and the contracts that the company has made with them. It also keeps contact data for each of these companies. Because of all the data in the system, it is the reason that the company will be affected by the GDPR regulation that has gone into effect on May 2018.

3 INTRODUCING GDPR

[2] GDPR is a regulation that was passed in the European Union and will take effect on May 25th 2018. The purpose of the legislation is to empower data subjects (users of services that collect the users' personal data) to have more power over how their personal data is stored and processed. (1) The regulation claims that it is a fundamental right to protect people from processing from their personal data, referring to Article 16(1) of the Treaty on the Functioning of the European Union and Article 8(1) of the Charter of Fundamental Rights of the European Union.

Everyone has the right to the protection of personal data concerning them. – Article 16(1) of the Treaty on the Functioning of the European Union

Everyone has the right to the protection of personal data concerning him or her. – Article 8(1) of the Charter of Fundamental Rights of the European Union

GDPR requirements include giving some power to the company's customers and contacts to decide how their data is used in the company's systems. It also requires private companies to set up proper security strategies to prepare for possible data breaches. Failure to meet the requirements of the regulation may result in a fine of up to 4% of the company's annual turnover.

The regulation introduces some words and terms, the most important are:

- **Personal data** is information that can identify a person. A person's real name is the most common identifier, but personal data can also be a group of other information that can be used to identify a person when there is enough of it.
- **Processing** means any operation that is used on personal data. Creating, modifying and deleting personal data falls under processing, and so does reading personal data for an operation that needs it.

- **A data subject** is the person whose personal data is being processed.
- **A controller** is the one who makes the decision to process personal data and the reasons why they are doing it. For this thesis, the company Konecranes is a controller.
- **A processor** is someone actually doing the processing, for example an employee or a contractor of the controller. For this thesis, an employee working for Konecranes is a processor.

3.1 Data subjects' rights to their personal data

(Article 17) GDPR grants data subjects the right to access their personal data and to have it removed from the data controller's systems if the personal data is no longer necessary to fulfill the purpose that the data was originally submitted for. The data removal ability is known as the right to be forgotten. The data subject also has the right to know what their personal data is used for.

(Article 20) In addition to simply being able to access their data, the data subject must also be able to retrieve their personal data in a format that allows the personal data to be easily transferred to another similar service. The regulation calls this data portability. The regulation even suggests the ability to transfer the personal data directly from one controller to another, but the sentence begins with "where technically feasible" making it less of a strict requirement.

(Article 21) In cases where personal data is processed for direct marketing, the data subject has the right to object to processing like that. The data subject must also be informed of this right separately from other information. This means that the information that when the user is informed of the right to object from marketing, this information must not be hidden behind a long "terms and conditions" document.

The right of a user to their personal data is the most important right granted by GDPR and is often the cause for most changes to be done in IT systems. Personal data can be stored in

a format that makes it difficult to retrieve, making it more difficult to adhere to this part of the regulation. Systems may have to be re-made in a way that allows such data retrieval to be possible.

3.2 Notification if a breach occurs

(Articles 33 and 34) GDPR mandates that in the event of a personal data breach, data subjects must be notified of the breach having happened within 72 hours of the data controller becoming aware of the breach. If the notification cannot be sent within 72 hours, the data controller must send an explanation for the delay along with the notification.

This notification must contain at least the following information:

- What parts of personal data has been breached
- Approximately how many data subjects are affected
- Contact details of the data protection officer
- Description of the likely consequences of the breach
- What the controller will do from this point on to help with the situation

The purpose of such a notification will be to warn the user that some of their data is out there so that they can take the necessary precautions. The notification should also contain information on what problems may be caused by the data breach and what precautions the data subject can take to mitigate the damage. For example in the case of a password leak (even if the password is hashed in the data) the data subject must be instructed to change their passwords in all services where the same password has been used.

3.3 Privacy by design

(Article 25) Data protection must always be one of the priorities when making changes to systems or developing new systems. The data controller must implement all possible measures to protect the rights of data subjects. Pseudonymisation and data minimization

have been provided as examples. Personal data must not be made accessible to an indefinite number of people.

The Information Commissioner's Office in the United Kingdom [3] interprets this part of the regulation as requiring data protection to be considered during the design stage of building new systems. Therefore data protection must always be discussed during the design portion of the systems development life cycle.

3.4 Data Protection Officers

(Articles 37-39) A controller must designate a data protection officer. This is a new role that must be fulfilled in order to be compliant with GDPR. Their job includes training employees to be compliant with data protection requirements, maintaining data processing records within the company and telling data subjects about their rights to access and be forgotten. They are the ones who ensure that the entity they are working for is GDPR compliant and will be cooperating with supervisory authorities if their attention is needed.

While obtaining consent from data subjects to process and store personal data, the data subject must be informed of the identity of the data protection officer who they can contact in case they have questions about the data protection policy. The data protection officer must also be available to help in case of a security breach that causes the data subject's personal data to leak out.

3.5 Member State specific authorities

(Article 51) Each European Union member state will have their own supervisory authority that will take complaints about GDPR compliance. The supervisory authority is also in charge of data processing inside public authorities and will ensure that the processing happens according to the regulation. Member states can also have multiple supervisory authorities if required so that the implementation follows the existing constitution of the country and fits in to the country's organizational structure. If multiple supervisory

authorities exist in one member state, one of them needs to be a single contact point to ensure smooth cooperation between member states' supervisory authorities and the European Commission. (Article 52) The supervisory authority must be independent from any external influence and should not take instructions from anyone. Member states must ensure that the supervisory authority has all the resources that it needs to fulfill its duties.

In Finland, where the case company is located, the supervisory authority is the Office of the Data Protection Ombudsman, or "Tietosuojavaltuutettu" in Finnish.

4 DATA PRIVACY AND GDPR RELATED LITERATURE

This chapter will go through various data privacy related and GDPR related academic writings that have been made.

[4] Privacy is getting a worse reputation over time as Julie E. Cohen had found. Recent world events have caused the popular opinion to favor legislation for more surveillance by law enforcement, thinking that it will provide more security. The feeling of being safe and secure becomes more important than the freedom of not being watched.

The general public has also shown to favor convenience over privacy. The entire business model of modern social media is based on collecting information on people that they are willingly sharing in order to have that shared information seen by other users of the service. In addition to the actual purpose of the service, the data can be used for targeted advertising. Search engines also take into account the web sites that the user likes to go to, allowing for personalized results – even if the user does not consent to such data collection. This is quite different from the previously mentioned government surveillance, as these are all actions taken by private companies. Giving up privacy provides people services that they find convenient and therefore the privacy violations are not seen as intrusive.

Another argument against privacy concerns is the idea that if you have nothing to hide, there is nothing to fear. [5] Daniel J. Solove from the George Washington University Law School has criticized this idea, and would ask anyone who says they have nothing to hide to show everything they have.

The concern about privacy and personal data has led to the creation of the GDPR.

4.1 Possible effects of GDPR

[6] Giovanni Buttarelli in the International Data Privacy Law journal believes that the GDPR will end up becoming a standard around the world. “Over half the countries in the

world now have a data protection and/or privacy law, and most are strongly influenced by the European approach". This makes Europe a front-runner in data privacy and it is expected that other countries will eventually come up with a similar GDPR of their own. If that happens, European companies that are already compliant with the law may get into an advantageous position as they've already done the work needed to comply with the EU version of data privacy.

[7] Graham Greenleaf the Professor of Law & Information Systems at the University of New South Wales sees the GDPR as a step at adopting a modernized version of Convention 108 of the Council of Europe as a global standard. This convention is meant to protect individuals from automatic processing of personal data. He divides data privacy laws into "generations" where the 1995 EU directive (the predecessor of GDPR) is a 2nd generation of data privacy standards that had slowly become adopted worldwide even outside Europe. The GDPR marks the arrival of the 3rd generation that includes rights of data subjects to have control of their personal data that is held by someone else. He believes that while other nations are unlikely to pass an entire GDPR-like bill, they will update their data protection laws to include some rights that GDPR is granting.

[8] Jesper Zerlang, CEO of LogPoint sees GDPR as an opportunity for businesses to make privacy a main concern in their operations and sees its passing as a milestone for cybersecurity. The threat of a large fine would encourage organizations to improve their data security even if the improvements had a high cost. In addition to this, the organization must store their data in a streamlined way in order to comply with requests to obtain someone's personal data quickly. In short, Zerlang is optimistic that GDPR will force businesses to come up with a proper strategy to store their data in a secure and organized way, making it easier to use the same data in the future in an innovative way.

4.2 Criticism of GDPR

Diker Vanberg criticizes the GDPR's ruling that requires data controllers to give out personal data in a format that can be transferred to other similar services. [9] He argues

that not all data can be transferred over somewhere else, citing Inge Graef [10] who gave the auction website eBay as an example. As part of the right to access, eBay is required to give reputation data that shows what kind of reputation the user has built on the website from positive or negative user ratings, but this is the kind of data that cannot be easily transferred over to another auction site. As noted by Graef, GDPR only gives the data portability right in cases where the transfer is "technically feasible and available". This can be interpreted in many ways and will most likely be used by companies to their advantage as they can simply claim that it's not possible. Users will still be able to get a copy of their data and be able to use it on another service, but there are other issues in simply copying data over to a similar competing service.

If an online service is a platform that involves interacting with other users, these interactions cannot be transferred over without the permission of the other users as well. In the eBay example, other users that have given the positive or negative rating are involved and they may not have given consent to move their ratings elsewhere. Vanberg also gives another example of a photo on Facebook that includes multiple tagged people on it. Even if the data subject (who is using the data portability right) appears on it, other people on the picture most likely have not given permission to anything. GDPR itself has noted this issue on Article 20, paragraph 4, with a statement that other persons' rights cannot be infringed. For any online service that involves interacting with other users, the data portability right is almost useless.

[11] Colin Tankard, director of data security company Digital Pathways has examined the effects of GDPR in the June 2016 issue of the journal Network Security. He notes that one of the requirements – the mandate to notify authorities of breaches within 72 hours – has not been done anywhere else before and calls the requirement "onerous". Other parts of GDPR are also criticized as the regulation leads to increased cost for businesses to implement parts of it.

[12] Kärt Pormeister. PhD candidate at the University of Tartu wrote an article criticizing the "research exemption" in Article 9, section 2 of the GDPR. According to the article,

GDPR does not define “research” well enough and may allow for private entities to claim an exception to process some data without the data subject’s consent. The risk would be especially high when it comes to pharmaceutical companies using patient data for research with the patient having given consent to nobody other than their doctor.

5 GENERAL GDPR COMPLIANCE IN KONECRANES

This chapter will go through the general GDPR compliance steps that will be taken that affect the entire company's IT operations. These are not related to a specific IT system, they are full company-wide initiatives.

The GDPR compliance project is set to be done in two phases. The first phase will be completed before GDPR takes effect, but the second phase will still be in progress at that point. The GDPR project was started very late – initial documentation is from November 2017, giving the company only six months to complete all GDPR compliance requirements. This deadline will not be met, but by doing the project in phases with the most important applications updated in Phase 1, the deadline can still be met for the largest amount of personal data that exists in the system.

The target was set to have the highest priority applications GDPR compliant by April 30th, completing Phase 1 by that deadline. GDPR required compliancy by May 25th. The highest priority applications process the most significant amounts of customer contact data. Applications with only a few users are considered to be low priority applications that are anticipated to have a low volume of requests which can be fulfilled easily. These applications have been relegated to be completed during Phase 2.

The GDPR regulation has caused the following new requirements to be applied to customer and contact data:

- Collection of consent to handle personal data
- Ability to receive data protection requests
- Restricting contact data from being processed upon request
- Removing contact data records if requested to remove
- User's right to get a copy of all of their personal data upon request
- Ability to opt-out from marketing, some countries require opt-in

- Defined access rights (must be clear who and why has access)
- Data security testing
- Cookie banner on Konecranes web sites
- Data minimization

5.1 Contact data handling

Contact data is data that is used to keep in touch with a representative of a customer or supplier. The data consists of persons' names, phone numbers and email addresses that are associated with companies. The GDPR considers this to be personal data because a name, phone number and email address combined with the company that the person works for can be used to identify a person even if they had another email or phone for personal use.

5.1.1 Centralized contact data database

To help with completing GDPR requirements, Siebel will become a centralized place where all contact data is stored. This decision was made because Siebel is highly customizable and is already a key part of Konecranes' customer relationship management process.

A centralized contact data database will drastically reduce the number of applications where contact data is maintained. By having all the contact data in one system which is integrated with others, it becomes easier to process the numerous data processing requests that may possibly be received once GDPR goes in effect. When data is located in numerous systems, it becomes difficult to ask each system's administrator to check if a user is there and fetch the data when needed. The GDPR regulation requires all personal data requests to be done within one month, but if all the data is stored in one location a request can be processed in only a couple of minutes after a person's identity is confirmed and the request has been approved.

When contact data has been centralized, new application capabilities to handle all contact data processing must be implemented. All applications that store contact data in some form

need to be integrated with the contact database in Siebel (Siebel FS is naturally integrated in Siebel CRM as they are the same application – the distinction between these two is only made through views visible to end users). The end goal is to remove all manually kept contact lists and have all contact data easily accessible in a single location, ensuring that nothing is missed when a request to take some kind of action (retrieving, modifying, locking or deleting) to a person's data is being processed.

Konecranes in Figure 2 provides an example of such integration. Arrow towards Siebel means that the application can send data towards Siebel and have it changed in there, and an arrow away from Siebel means that Siebel can send data to the application and have connected contact data changed in there. If a system is capable of accepting new submitted data, it must be able to send it to Siebel. If a system is capable of storing contact data and doing this is required for it to function, it must be able to receive it from Siebel. When any user of any Konecranes system enters contact data, it must be present in Siebel in some form and the integration must provide alerts to administrators if the data sharing process fails for any reason.

This central contact data integration will not be completed in time for GDPR as it involves all of the contact data that has ever been collected and takes development time for multiple applications. An alternative process to complete requests will be utilized while work on the integration is in progress.

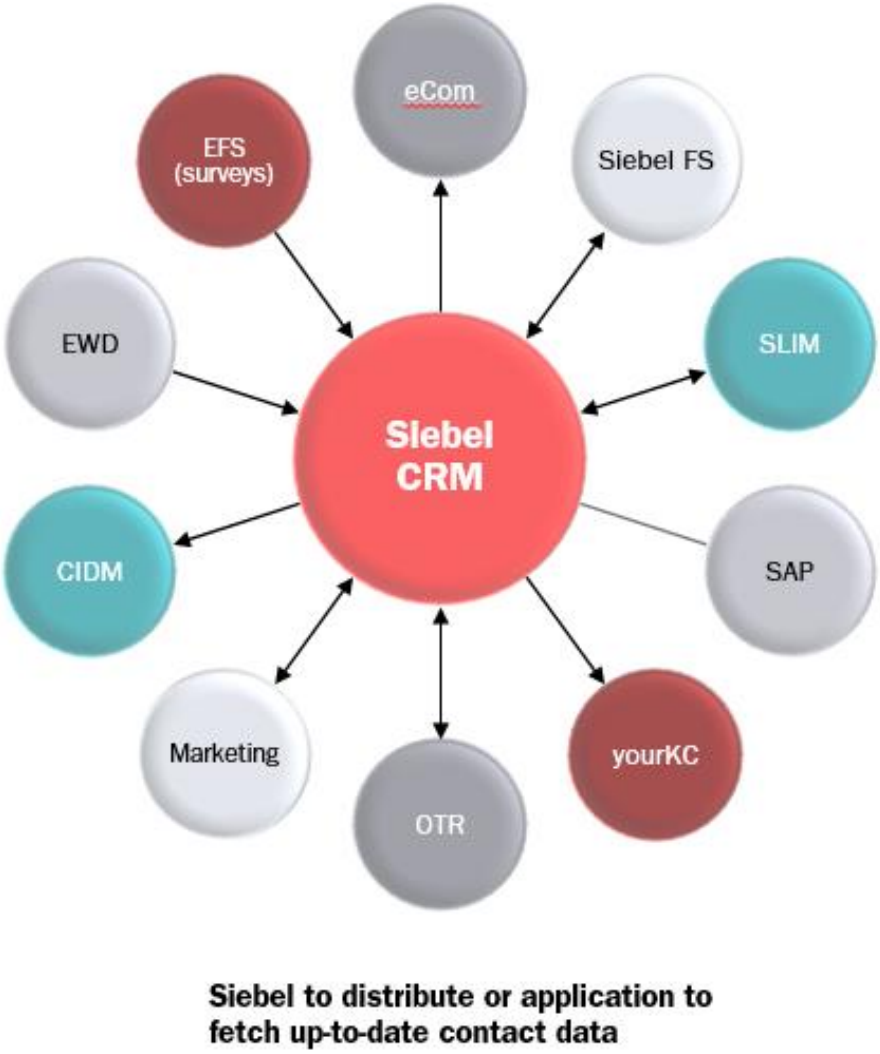

Figure 2: Siebel as a contact data master

5.1.2 GDPR queue in helpdesk

A new email address and a new support web form will be set up, which will create a ticket in a separate GDPR queue in the customer service system. It is especially important to keep track of data requests because GDPR requires responses to data processing requests within 30 days. When a data protection related service ticket is created (either through a web form created for this purpose or through a general help desk ticket that is identified as a data protection request), it will be sent to the Data Protection group to validate whether or not the request is valid and which applications the requester has used. When the request has been validated and the applications have been identified, the request will be divided

into sub-tickets that will go to application-specific support where they will perform the required tasks.

The act of dividing a ticket into sub-tickets for various system administrators is a temporary measure until the Siebel integration is complete and contact data can be found easily in one place. The process that is followed for data protection requests will be detailed more thoroughly in Chapter 8.

5.1.3 Cookie banner

All Konecranes websites must be able to display a banner warning the user that the website uses cookies along with a link to the official Cookie Statement on the Konecranes website, and an OK button that the user can click to show that they have seen the banner and have consented to the use of cookies. The cookie will store the time and date when the OK button has been clicked.

The banner will be implemented on both external (open to the public) and internal (accessible by employees) websites. The cookie statement will be separate for both.

5.2 Employee data handling

Employee data will be processed according to a basic guideline. Employee data can be stored and processed only as long as it is needed to fulfill employer duties, which includes paying salaries, managing insurance and healthcare, saving documents like tax information and allowing support services like login management. Employee data may not be collected for any other reason, and excess employee data must be deleted if the employment ends.

Employees inside the European Union were required to sign a consent agreement that lists the personal data that Konecranes will process for employment purposes. Therefore in order to continue working, employees are required to give their permission for the company to store their employment data for the aforementioned purposes. Employees that are outside the EU or other countries with a GDPR-style regulation are not required to sign

a separate consent form – they will agree to have their data stored in their regular employment contract, which has been the custom so far. The full process that a new employee (or an employee whose data needs to be updated) has to go through is shown in Figure 3. Whether consent is needed depends on if the employee is in the EU zone (under GDPR) or not.

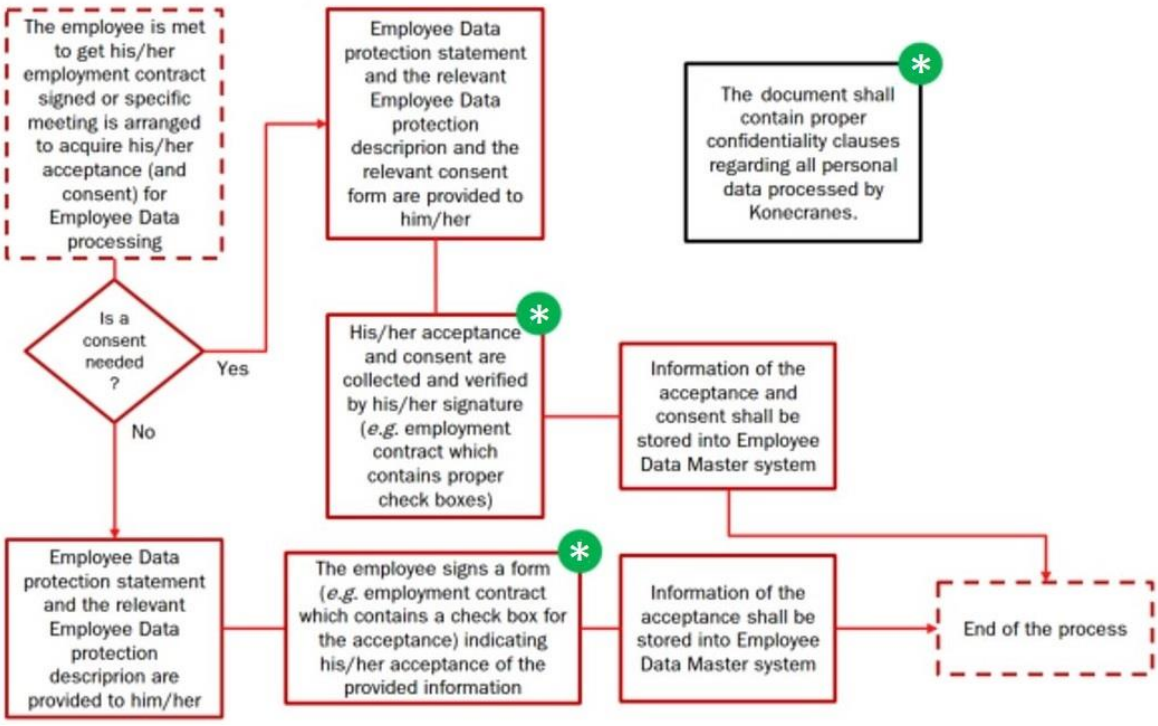

Figure 3: Process for processing new employee data – consent is needed for EU-zone employees

5.2.1 Updating and archiving of employee data

Keeping updated personal data such as current address and bank account for salary payment is considered the employee's responsibility. The employee can use their personal Konecranes username and password to log in to the People system where personal information can be changed. The agreement recommends that this is the method used for the employee to access and update their data, but the data protection team can also be reached by email or a web form.

After an employee stops working for the company and reaches end of employment, any leftover employee data will be archived and will no longer be accessible in UIs of systems that process employee data. These archives will be kept for a set retention time and will be deleted afterwards. The retention time has been agreed to be 10 years and the countdown to delete older data will start counting from April 30th 2018, the date when the company has mandated GDPR compliance. Therefore old employee data will start to automatically be deleted on April 30th 2028.

5.2.2 Mandatory two-step authentication for remote work

It is mandatory for all employees to enable two-step authentication to access Konecranes resources remotely. Two-step authentication is a technique to make it so that a username and password are not the only details needed to logged in and that the user must provide extra proof that they are the user that they claim to be.

The two-step authentication method in use is Microsoft Authenticator, because Konecranes uses Microsoft technologies to protect its internal sites. Microsoft Authenticator is a mobile application that should be installed on the employee's work phone. If the user logs in from a new computer (verified by there being no existing access token in a cookie) they will also be prompted to press the "Accept" button on the application.

In addition to Microsoft Authenticator, another two-step authenticator app is in use in order to allow users to access the Konecranes VPN (virtual private network). The VPN is used to access the Konecranes internal network remotely. Being in the internal network either physically or remotely via VPN is the only way to access testing and development environments and some internal processes used in development.

5.3 Development practice change: Privacy by Design

One of the biggest regulations in GDPR is privacy by design. According to Article 25 of the GDPR, data protection must always be considered a priority when a new system or changes to systems are developed. On the software development life cycle this will take

place during the design part. Konecranes uses the Jira tool to track the status of software development, and the Jira steps in which privacy by design is applied is shown on Figure 4.

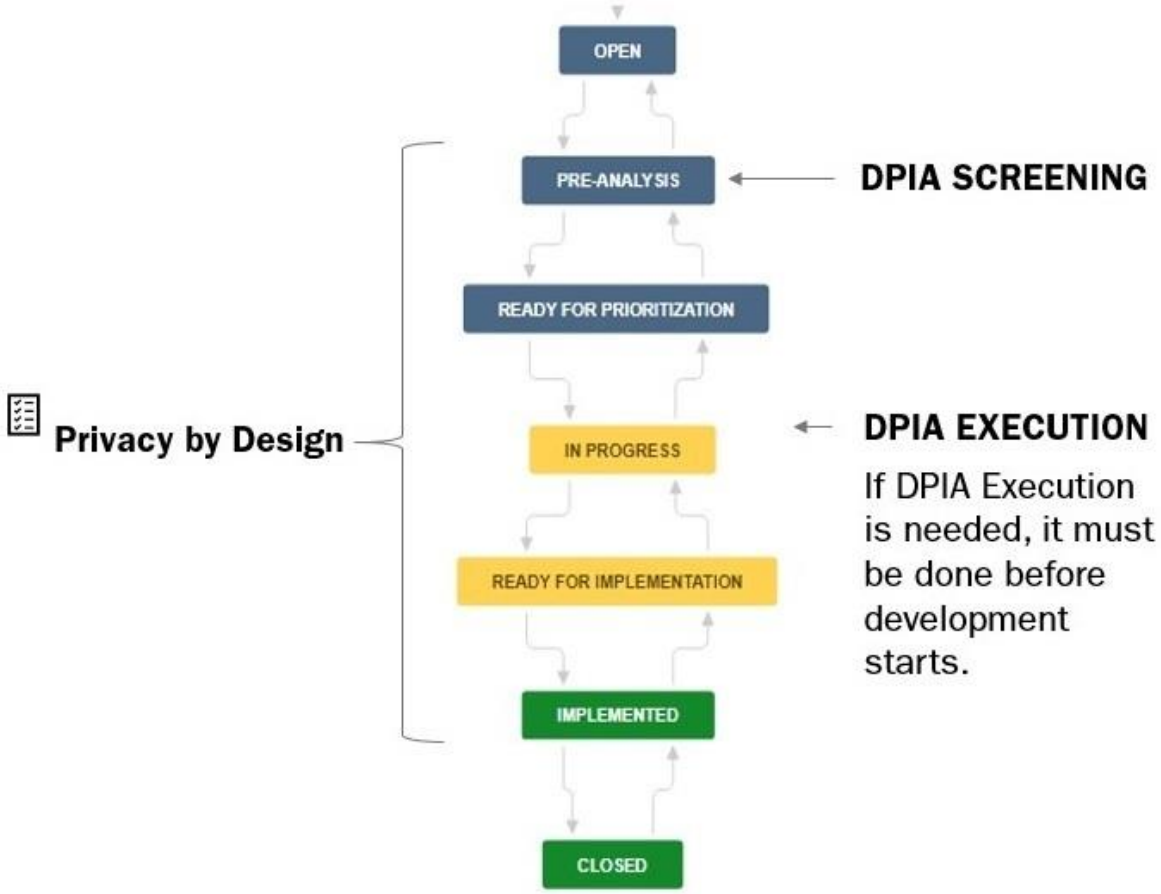

Figure 4: Privacy by Design and Jira steps

Data protection requests are considered to be "non-functional requirements" that have to always be taken into account in service development. Before any new developments are done, the development team must perform screening to determine whether a Data Protection Impact Assessment (DPIA) must be executed. If it is determined that a DPIA is not needed, the Data Protection Manager will still be contacted with a report that details what is being done and why the DPIA was not needed.

Whether DPIA is required is determined with a questionnaire. This is known as DPIA screening. The following questions need to be answered with yes/no:

- New personal data processing technology involved in the IT system. If yes, DPIA required.
- IT system used for systematic monitoring of publicly accessible areas. If yes, DPIA required.
- IT system used for systematic and extensive evaluation of personal aspects leading to decisions producing legal (or similar) effects to data subjects. If yes, DPIA required.
- IT system related data processing belonging to an official list of data processing operations requiring DPIA. If yes, DPIA required.
- Amount of data subjects of various types (numbers).
    - Customer contact data
    - Vendor contact data
    - Employee data
    - Employee candidate data
    - Other personal data (if this is not zero, DPIA required as a new personal data category is introduced)
- The geoscope (how many users are affected) of personal data processing. This is combined with later questions to determine DPIA requirement.
    - Single country
    - A continent
    - Global
- Special categories of personal data. If any of these are checked and the geoscope is a continent or global, DPIA required as it is considered to be processing of sensitive data on a large scale.
    - Data revealing racial or ethnic origin (photo)
    - Political opinions
    - Religious beliefs
    - Trade union membership
    - Health data
    - Criminal record data

    - Biometric data
    - Location data
- What the data is used for (list of various purposes that personal data is currently used for to tick yes/no). If the field “other, please specify” is ticked, it counts as a new purpose and it requires a DPIA.
- Nature of data processing. If one or both of the last two are checked and the geoscope is a continent or global, DPIA is required as it’s considered to be large scale processing affecting data subjects intrusively.
    - Has no effect on the data subject
    - Has back-end effects that aren’t visible to the data subject
    - Affects data subjects collectively (a group decision can be made with this data)
    - Affects a data subject individually (affects someone personally, for example data can be used to decide a job task change or whether someone is to be hired or not)

When the information is filled out into a template spreadsheet, it is automatically decided whether DPIA is required or not. DPIA is needed if the new system includes new personal data processing technology. This includes new algorithms for profiling individuals, new methods to identify users based on existing personal data or any technology that requires additional personal data to be collected that is not on the system already. Additionally, the data subjects that the new technology affects must be in the EU area because the GDPR is only in effect there.

The DPIA itself will be carried out by the Data Protection team. The team will ensure that all measures to protect the data subjects’ rights are carried out during the development of a new project. The Data Protection team will also determine if these new actions are completely necessary and will try to seek alternative methods to carry out a task that does not require processing as much personal data. The Data Protection team will eventually decide if the new project will get greenlit or not.

Even if DPIA screening results in no DPIA getting performed, the questionnaire will work as official documentation to prove that Konecranes has considered data protection as a requirement in all of its projects and therefore followed the regulation properly. The actual DPIA will be done by the Data Protection team and they will determine whether or not to interfere with the new system's development, or if the project is allowed to go live in the first place. If DPIA screening or DPIA execution has been performed but there is a later a change in the design plans of the project, screening (and execution if needed) must be performed again. Screening does not need to be performed again if a new implementation of a project is done with the same design (for example, bug fixes).

6 INTRODUCTION TO SIEBEL

Siebel is a customer relationship management (CRM) application that is currently owned by Oracle. It was originally developed by Siebel CRM Systems, Inc. that was founded in 1993 by Thomas Siebel and Patricia House. Oracle bought the company in 2005 and made Siebel its brand name.

In the Siebel CRM application, sales persons can update and search information about Konecranes' customers and partners. It makes customer and partner data easily and consistently accessible across the organization. Sales persons are provided with a common way of recording sales cases, and top-level management is given easy access to analyze sales case data efficiently.

Konecranes uses the Siebel Field Service version of Siebel. It allows salespersons to record agreements and to create service plans for any purchased products. A custom made Preventive Maintenance Engine (PME) will generate new work for a technician to perform as agreed to in a maintenance plan.

Siebel also has a Field Service side that is used by service technicians. The back office assigns work to technicians via Siebel and the technicians will accept work, record their actions and mark the work as complete when they are done.

6.1 Siebel data structure

When a user is looking at the Siebel web application, they are looking at one of many views. A view shows the user one or more applets, and it is the main way that a user will interact with the Siebel application. An applet is a graphical user interface that displays the content of a business component to the user and allows the user to modify the information if they have the rights to do so. Applets in a single view can work together, the most prominent example being a list applet that lists records and a form applet that displays

more detailed information (the form applet has more fields than the list applet) when the user highlights a record on the list applet. An example of a list applet combined with a form applet is shown in Figure 5.

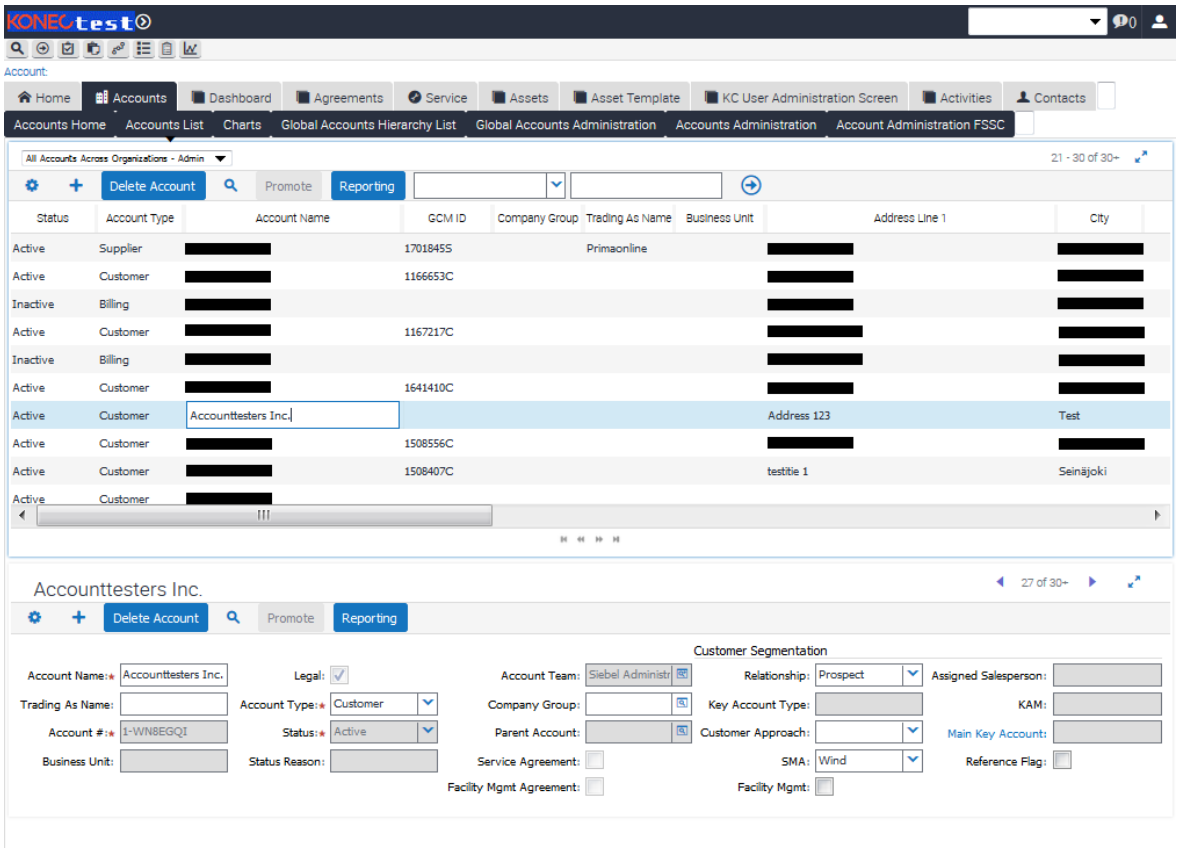

Figure 5: a list applet and a form applet in a view

An applet displays data from a business component. A business component takes columns from multiple tables into a single structure. A table is simply a table in an SQL database and can be viewed and edited with normal SQL client software.

Siebel users are given one or more **responsibilities** that determine what views the user has access to. This is used to hide unnecessary information to help the user to focus on the task that they are hired to do and is also how data is restricted from users who are not meant to have access to it.

Official Konecranes documentation makes a difference between Siebel FS and Siebel CRM. These two are the exact same Siebel application, but the difference is made by having Field Service users have different responsibilities from CRM users, which makes the application look entirely different depending on who is logged in. A field service technician is only capable of viewing service requests that belong to the branch that they are working at, and has no visibility to the agreement that created the service request.

6.1.1 Account

When Konecranes gets a new customer or supplier, they will be added to Siebel as an Account. An **Account** is a record of a company in Siebel, and it can be either a "legal company" or a "business area". A legal company is the legal entity of a company that is recognized by law and is distinct from other companies. In some cases a legal company can have multiple addresses where it is active and the other addresses will be added as separate accounts in Siebel, called business locations. A business location must always have a legal company that is considered its parent company, creating a hierarchy where there is one legal company with many business areas. A business area cannot be a parent of another business area.

Customer account data is created and updated inside a separate application outside Siebel known as Global Company Master (GCM). Integration between Siebel and GCM will keep the account data automatically up to date. When an end user wants to create a new account, they will have to contact a local requestor – different Konecranes branches in different countries have their own local requestors. The local requestor must check Siebel and GCM if the customer exists already. If it doesn't, the local requestor will check that the new customer is eligible for business (credit check), and then they will contact the Master Data Maintenance (MDM) team in the Financial Shared Services Center (FSSC) to add a new customer record to GCM. The MDM team will verify the new account data for the following:

- Check again if the customer already exists in the GCM application. If it exists, verify with requestor
- If the new customer is a business location, it must have a legal company as its parent
- Verify that the customer exists in official trade registers or has a D-U-N-S number (unique 9-digit identifier for business)

6.1.2 Organization

Organizations are hierarchically sorted region data in Siebel, which are used to separate data regionally and prevent employees from seeing data from regions that they are not working in. Users and Accounts are tied to Organizations.

Organizations come in the following levels:

- Brand
- Region
- Sub Region 1 (exclusively used by EMEA)
- Sub Region 2
- Area
- Sub Area (US only, divides USA East and USA West)
- District
- Branch

The highest level Organization is a Brand. Brand data is used to separate Konecranes branded activity from other brands. While Konecranes owns SWF Krantechnic and R&M, they are autonomous companies whose actions do not impact the business of Konecranes itself. These non-Konecranes brands are known as Alpha brands.

Accounts outside the United States are tied to region level Organizations, while Accounts in the United States are tied to District level Organizations that represent a collection of states in the U.S.

For an example of the hierarchy present in organization data, the branch “FI50_Korjaamo” can be reached this way:

- Brand: KC_Global
- Region: EMEA
- Sub Region 1: North EMEA
- Sub Region 2: North East Europe
- Area: Finland
- Sub Area: (N/A, only used by USA)
- District: Finland – District
- Branch: FI50_Korjaamo

Each user has a “division” field where the organization is set. In addition to deciding what area’s data the user has access to, it also sets the scope of the data that the access is for. For example, if the user’s division is EMEA, they have access to all data in the EMEA region, including each country. If the user’s division is a branch, for example the above FI50_Korjaamo, they only have access to data in that branch. Branch level is only used for service technicians who work in that branch. Back office work and other administrative work are done at a higher level.

6.2 Field Service

The Field Service side of the Siebel application covers service agreements and all information needed to perform work on the go. Field service data is tied to the same Accounts as CRM data. The data structure for field service related data is shown in Figure 6.

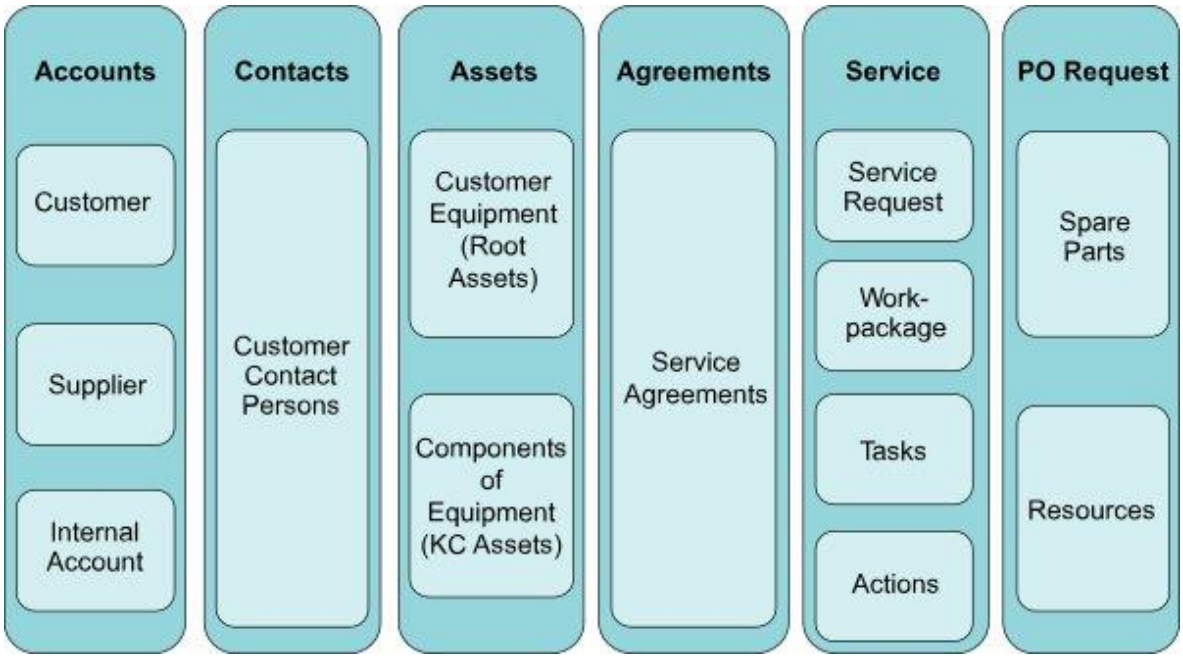

Figure 6: Siebel Field Service data structure

6.2.1 Agreement

A service agreement (only called Agreement from now) is an object that records which service products have been sold to a customer and what its conditions are. It contains the service programs, which assets the service is meant to be performed on and how long the agreement lasts.

Using the service product and asset information present in an Agreement, the Konecranes custom made Preventive Maintenance Engine (PME) will automatically run nightly and create new Service Requests for the Agreement.

6.2.2 Service Request and Workpackage

A Service Request is a collection of tasks that a field operative needs to perform. These tasks are called Workpackages. Service technicians will have different Service Requests assigned to them. In their daily work they accept workpackages, perform the tasks that are in them and then mark them as complete.

A branch manager can assign Service Requests to a technician through a Planning Board. The planning board lists all technicians that the branch manager has authority to assign work to, and shows in a calendar view when these technicians are free and when they're busy (already have work assigned for that day). When a Service Request is assigned to a technician, they will be able to record what they have done into the Service Request using either a mobile app or a Web view via a laptop (depends on country).

Service Requests also have a customer contact assigned. This is the person the technician is meant to meet at the work site and whose signature must be received to finish work.

6.2.3 Asset

An Asset in Siebel is an object that refers to a piece of equipment or machinery. These items may have been sold to the customer by Konecranes or the customer may have bought the item from another seller but has made a service agreement with Konecranes. Because Assets always belong to a customer, they are created under a customer Account.

Assets can have subcomponents that are other Assets, creating a tree of Assets. The top of the asset tree is the complete piece of equipment that all subcomponents are connected to and is called a Root Asset. The subcomponents are called KC Assets.

Some of the Assets in the system are Asset Templates, which are used to quickly create a new asset based on a product that Konecranes sells. When an Asset is created through one of these templates, the entire asset including all subcomponents will be copied as a new Asset under an Account. Asset templates are not attached to any Account.

6.3 CRM

The CRM (customer relationship management) side of the application focuses on the actions of sales persons. When they have a new Account created in the system, sales persons will record their actions into Sales Cases that will keep track of sales opportunities and if Koncranes has successfully made a sale or not.

6.3.1 Sales Case

A Sales Case is an object that records and tracks sales opportunities through various stages. The sales stages are the following:

1. Registered Lead
2. Qualified Lead
3. Opportunity
4. Qualified Opportunity
5. Offer
6. Hot Offer
7. Order Received

As a sales case advances further, more data is required to be filled over time. On the first stage only a simple name for a sales case is needed, while on the seventh stage there is a full order and the sales case has full data of what has been purchased and when.

For this thesis, the most important stages are the 2nd stage where the company's information is entered along with a lead contact and the 3rd stage where the name of the customer contact is entered. These are names of people which are considered to be personal data as far as GDPR is concerned.

6.3.2 Contact

Contacts are people who can be contacted to do business with a customer or supplier. A new contact is added to an Account as part of a new Sales Case or a new Agreement when a CRM user is working to get a new business deal for Konecranes. Contact data items are personal data of real people, making it the most important part of Siebel that gets affected by the GDPR.

Contact data stored by Konecranes includes the person's first and last name, email address and phone number. There are also fields for street address and zip code, but normally it's only the location of the company they are working for that will be copied there. A contact

data item is always connected to an Account, as there is no need to store any information of people who aren’t affiliated with a company.

An Account can have multiple Contacts, but Agreements and Sales Cases can only have one. Therefore having multiple Agreements and Sales Cases is the primary reason for an Account to have multiple contacts.

7 CHANGES SPECIFIC TO SIEBEL

Because Siebel is considered to be the customer contact master, Siebel is going to be the most important application in Konecranes IT for the amount of contact data (considered to be personal data) that is getting collected in it. Therefore the application is part of phase 1 meaning that all of the following has been done by April 30th.

7.1 Automatic anonymization of contact data

GDPR requires old unused data to be removed from systems even if the data subject has not requested a deletion. The regulation does not specify the time that it takes for data to be considered old and unused, but within Konecranes it has been decided that this time will be 10 years. After old contact data has been unused for 10 years it will be either deleted or anonymized even if the contact has not requested for this to be done (if they want their data removed earlier, that can be done through a data protection request). Deleting contact data may cause issues with sales case and agreement data so anonymization will always be preferred. Anonymized personal data is fully overwritten with generic information that cannot be turned back into the original data.

In order to determine whether a piece of personal data is unused, a new database field is to be implemented that will store the date and time when the personal data was previously involved in an activity. The contact data will be automatically anonymized after more than 10 years has passed from this date. The following activities will update the “last update” date for a contact:

- Contact is created
- Contact data is modified
- A new sales case is created that this contact is involved with
- A new agreement is created that this contact is involved with
- A new service request is created in an agreement that this contact is involved with

7.2 No Marketing flag for Contacts and Organizations

A “No marketing” flag on a contact needs to be implemented to fulfill the GDPR requirement of requiring data subjects to opt in to receiving marketing emails. The script that sends automated emails will check for this flag before sending them, making it so that any user that has the flag set will receive no automatic emails of any kind.

In addition to adding a flag to contact data, another “No marketing” flag needs to be added to countries that have specific laws that require marketing consent from everyone that is added to the system as a contact. This is done by adding a flag specific to Organizations. When a new contact is created and belongs to an Account whose Organization has the no marketing flag set, the new contact will automatically have the no marketing flag set to themselves. The employee who added the contact’s data will have to ask for permission from the contact to manually remove the flag if this is the case.

For contact data the No Marketing flag is a Boolean value stored in a new column on the S_CONTACT table, which is the main table where all the contact data is. The date when this value has been modified will be stored as a DATETIME value and and the username of the employee who did the modification will be stored as a VARCHAR value in two other new columns.

A new script will be created on the New Record business component in the Contact Business Object. The Business Object will run whenever a new Contact is created. The new script will check whether the No Marketing flag is checked in the Organization of the Account that the contact will be part of, and automatically set the No Marketing flag if the Organization has its equivalent flag set.

The Organization level No Marketing flag is implemented similarly with three values: the flag itself, the user who set the flag and the date when the flag was set.

7.3 Restriction on data processing (data lock)

Contact data will have the ability to have editing locked. Similarly to the No Marketing flag, this will be implemented with three new data values: the status of the lock, the username of the user who activated the lock and the date when the lock was activated. When a contact is locked, the No Marketing flag will also automatically have to be checked because the data processing restriction applies to all processing according to GDPR, meaning that using the data for marketing will also be forbidden.

When user searches for contacts in any contact list applet, the list will not include contacts with the restriction active. This makes the contact nearly invisible for regular users – they cannot be searched but their names may still appear in sales cases and agreements. There will be a special GDPR View visible to administrators only that will include locked contacts in the search. That is also the location where an admin user is able to remove the lock.

7.4 Export Process for contact data retrieval

Part of GDPR requirements is to allow a contact to retrieve all of their personal data from the Siebel system. The process on how this request happens will be detailed more thoroughly in Chapter 8, but eventually the request will be given to Siebel administrators that will retrieve the data. The request process is also briefly shown in Figure 7.

There is no need to implement any extra features into Siebel to allow the retrieval of contact data. Instead, a set of SQL scripts has been provided and a system administrator will carry out the task. Microsoft SQL Server Management Studio allows copying and pasting the SQL request response straight from the SQL server software to a spreadsheet.

From the CRM side, if a user was to request their data, they will be provided a list of all sales cases where the user has been chosen as a Sales Case Contact or a Sold to Party Contact. In addition, they will be provided a list of all activities where the user has been selected as a contact person.

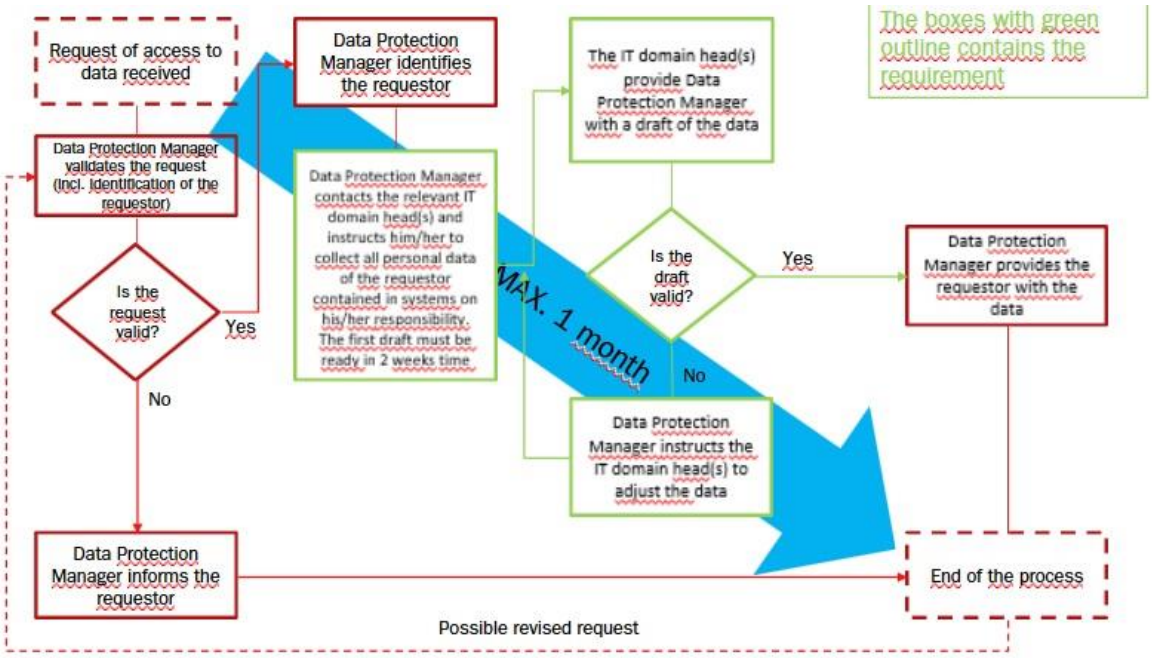

Figure 7: Data Protection request process

The SQL scripts will retrieve the following information:

- First and last name
- Phone number, mobile number, fax number
- Email address
- Preferred contact method
- Marketing Not Allowed status, yes/no
- Preferred marketing contact method
- Job Title, if used – this is rarely used
- Number of Activities that the user is set as Contact on
- Number of Agreements that the user is a Contact on
- Number of Charges that belong to Agreements that the user is a Contact on
- Number of Agreements that the user is a Sold to Party Contact on
- Number of Assets that the user is set as an owner on

- Number of Sales Cases that the user is a Contact on
- Number of Sales Cases that the user is a Sold to Party Contact on
- Number of Service Requests that the user is a Contact on
- Number of Service Requests that the user is a Sold to Party Contact on
- Number of Workpackages that the user is a Contact on

The detailed information inside Agreements, Sales Cases and Service Requests is not included in the data given inside requests. This is because the data is considered to be a contract between two companies and does not involve personal data of natural persons other than methods to contact them (work email and work phone). Detailed agreement data is also a trade secret and may be used by competitors to their advantage if they gain access to it. Because of this, only the number of items that the contact is involved in will be given. Companies that Konecranes deals with are expected to have their own bookkeeping where they record details on how much money they have paid and received and what products or services they have given or received.

8 GDPR REQUEST PROCESS

This chapter introduces the process of how Konecranes will handle GDPR-related data protection requests. The process is shown in Figure 8. The general high level process for GDPR related requests will involve a data protection group. Their task is to ensure that any upcoming requests are valid. The packaging of the data is left to application administrators, and each admin team has decided what they feel is the best way to handle requests quickly.

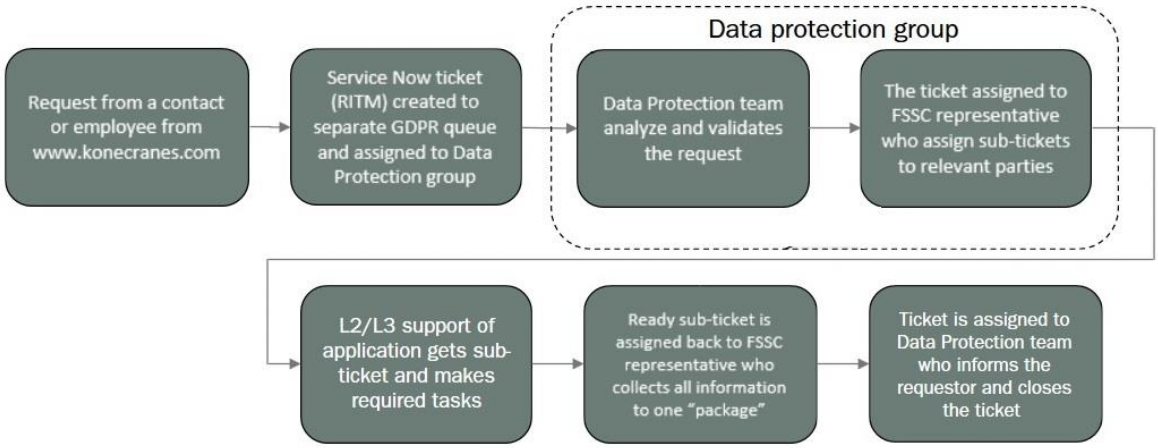

Figure 8: Data Protection request process

8.1 Web form for GDPR requests

The official method of gaining access to personal data is a web form that includes checkboxes for all the rights that a data subject has to their personal information. This will immediately inform the data subject of all of the rights granted by GDPR as they are given as a choice and allows the data subject to pick from a list what needs to be done with their data. In most cases the free text field is mandatory and the data subject must explain what specifically they want to have done. For self-explanatory requests like opting out of marketing or requesting a copy it isn't mandatory to fill in more information.

After they have chosen their right on the first part of the form (shown in Figure 9) the user will be told to fill in their basic personal information, which will be used to identify the

correct information that has to be processed in the system. Basic information includes the user's name, phone number, email and the company they are working with (all contact data within Konecranes is tied to company information). The user can also fill in optional information to make the data processing easier and faster – this optional information includes street address, postal code, city and country.

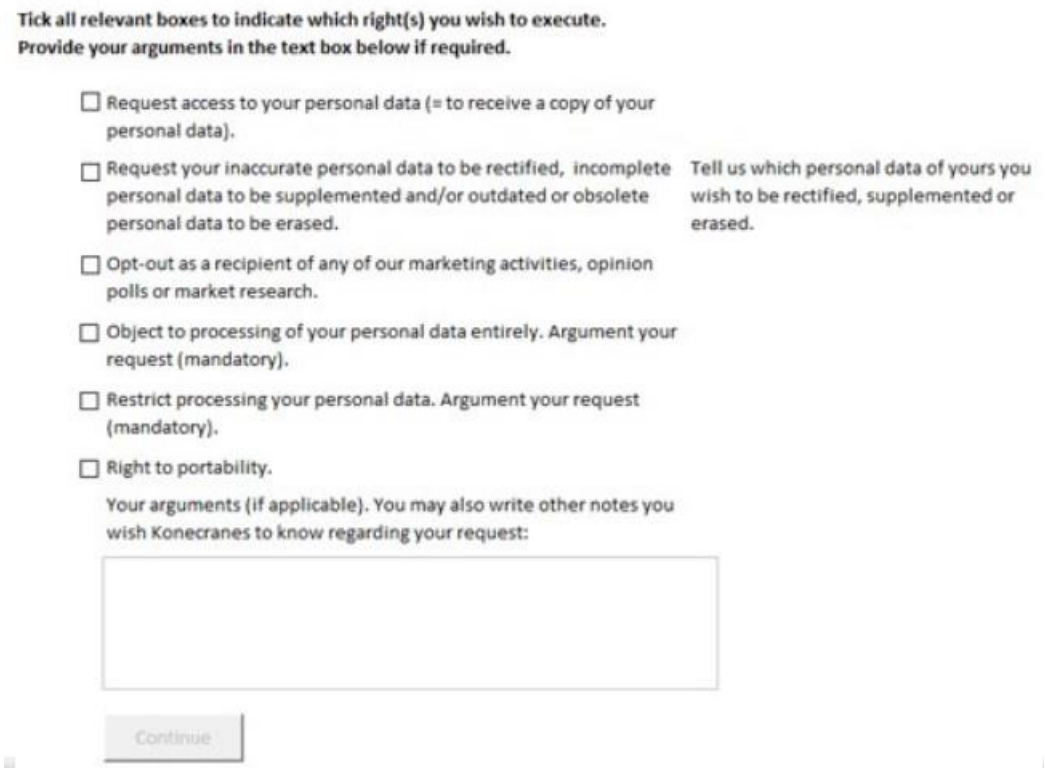

Figure 9: Screenshot of the GDPR request web form

In addition to building a new Web form to help with data processing requests, existing user modification forms need to be modified to add an option to opt in to marketing. Some countries (Poland and Cyprus) have chosen to implement the regulation in a stricter way that requires this. Although it is not a GDPR country, this opt-in will also be in place for China which is implementing a similar regulation.

8.2 Data Protection process

After the web form has been sent successfully, a new customer support ticket will be created. The Data Protection team (that has been appointed specifically for GDPR) will receive the ticket and start working on it. Their primary task is to determine if the request is valid and actually came from the source that claims to need their information.

In addition to verifying the source, the data protection team will get any other needed information such as country-specific regulations and legislations and instruct the administrators of all systems to carry out any required tasks for these as well.

When the request has been confirmed to be valid, the Data Protection Manager informs the Financial Shared Services Center to start the pre-defined GDPR process. The task of FSSC is to separate the data request support ticket to different sub-tickets and assign them to the administrators of the systems that have personal data. This allows the system administrators of all applicable IT systems to perform the requested actions to personal data their own way, which can vary from system to system. The export process for Siebel was detailed earlier in Chapter 7.4.

Once all administrators have executed their task, the sub-tickets will go back to the Data Protection Manager who will review the results. All of the data will be compiled to a single spreadsheet file and given to the requester. The Data Protection Manager may contact the requester for more information at this step as well, if there is need for it.

9 REFLECTIONS AND THE FUTURE

GDPR is a complicated regulation and getting full compliance can be difficult because some parts of it are up for interpretation. Konecranes only started the GDPR project six months before the law was to go into effect, which made the process even more difficult as there was a time constraint. However, because Konecranes primarily deals in the business-to-business sector, the threat of personal data leaking is smaller than on a consumer-facing company.

These are only the first steps taken to get basic compliance with GDPR for the due date. Phase 1 included all high priority applications that contained a very large amount of data. Phase 2, that includes lower priority applications, will begin development immediately to make the entire Konecranes organization GDPR compliant as soon as possible.

There were very ambitious plans on making Siebel the centralized contact database for all contact data handled by Konecranes. This is helpful for GDPR purposes because if someone requests something to be done to their personal data, it can always be found on Siebel, and the Siebel data will be connected to the user's personal data that exists on other systems. This is still in development, but because it requires integrations with every system and also requires the company to make final decisions on what systems to keep or remove, this will take a long time to do. For now, the company is GDPR compliant in a system by system basis, so the administrators for each IT system will have to retrieve the data separately. The amount of data protection requests made in the first three months of GDPR has been low, so while the current solution takes much manual work the situation is temporary and so far there have been no issues.

10 SUMMARY

The most important part of GDPR is the ability for an end user to get a copy of their data and have some kind of access to it. Basic GDPR compliance has been accomplished, and there is now a process to allow end users to request a copy of their data and get it removed if they are no longer part of any contract with Konecranes.

The company has a large project where all contact data will be connected to one system: Siebel. Integrations will be built between Siebel and any other system that requires contact data so that if a contact's data changes in Siebel, it will automatically change elsewhere as well. This will help with GDPR compliance as it will be easier to find personal data across the entire Konecranes IT infrastructure and perform any needed actions on it.

However, the centralization project is not done yet. For the deadline, GDPR compliance is achieved on a system by system basis. A data protection support ticket will be divided into multiple subtickets and the administrators of each system will retrieve the data and perform the requested actions.

The storage of customer contact data in Siebel had only a few changes done: the ability to lock contact data from any editing and setting up a No Marketing flag which prevents the contact email from being used for automated marketing emails. The process of getting a person's personal data is done via SQL queries. They are ready and data retrieval will be quick when they are used, but the centralization of all contact data into Siebel is not yet complete.

In the development of a new IT system, data protection will always have to be considered during the design phase. This is called "privacy by design" in GDPR. Konecranes is complying with this regulation by having all product managers to perform a Data Protection Impact Assessment if required, and send the results to the data protection team.

In some cases this may not be required, but then an explanation must be sent why this is the case.

REFERENCES

1. Konecranes. Our Approach to Crane Maintenance [online], Available from: <https://www.konecranes.com/service/crane-service> [Accessed 14th October 2018].
2. General Data Protection Regulation [online]. (2016). Available from: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> [Accessed 25th September 2018].
3. Information Commissioner's Office – Data protection by design and default [online] Available from: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> [Accessed 24th October 2018].
4. Cohen, Julie E., What Privacy Is For (November 5, 2012). Harvard Law Review, Vol. 126, 2013.
5. Daniel J. Solove (2007). I've Got Nothing to Hide and Other Misunderstandings of Privacy. San Diego Law Review. 44, pp.745-772.
6. Giovanni Buttarelli (2016). The EU GDPR as a clarion call for a new global digital gold standard. International Data Privacy Law, Vol. 6, 2016.
7. Greenleaf, Graham, International Data Privacy Agreements after the GDPR and Schrems (January 30, 2016). (2016) 139 Privacy Laws & Business International Report 12-15; UNSW Law Research Paper No. 2016-29.
8. Zerlang, Jesper. (2017). GDPR: a milestone in convergence for cyber-security and compliance. Network Security. 2017. Pages 8-11.
9. Diker Vanberg & Ünver, MB. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? European Journal of Law and Technology, Vol 8, No 1, 2017.
10. Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63.
11. Colin Tankard, What the GDPR means for businesses, Network Security, Volume 2016, Issue 6, June 2016, Pages 5-8

12. Kärt Pormeister (2017). Genetic data and the research exemption: is the GDPR going too far? International Data Privacy Law, Vol. 7, 2017.