Abstract

Successful protection of company data assets requires strong technological support. As many security incidents still occur from within, security technologies often include elements to monitor the behaviour of employees. As those security systems are considered as privacy-intrusive, they are hard to align with the privacy and data protection rights of the employees of the company. Even though there is currently no legal obligation for developers to embed privacy and data protection in security systems, by taking privacy-friendly design decisions, developers can play a significant role in the protection of employees. Especially since privacy by design is gaining momentum in Europe, but nonetheless, because privacy and data protection law results in several obligations for companies, and the non-compliance with data protection law is increasingly under fire, the need for companies to deploy privacy-friendly security systems, is growing. Hence, developers will also increasingly benefit from designing privacy-friendly security systems. In this paper the MUSES RT2AE was studied as an example of privacy-friendly development of a [...]
MUSES RT2AE v P/DP: ON THE ROAD TO PRIVACY-FRIENDLY SECURITY TECHNOLOGIES IN THE WORKPLACE

1. INTRODUCTION

The rapid expansion of information technology has many clear advantages. However, there are also associated risks. Companies are more vulnerable to threats following from cyber-attacks, and, as a result, they need protection.

Despite the attempts of many companies to highly secure their information resources, security incidents occur. It seems generally accepted that the major threat for company security will come from within. Security incidents regarding insiders\(^1\) – i.e. where employees are the root cause for information security failures – even exceed the amount of breaches where outsiders are involved.\(^2\) Especially in the situation where employees use their personal devices to access company documents, company networks are often at risk. Indeed evidence suggests that company data assets often get lost or stolen as a result of internal employee actions, whether or not it follows from intentionally malicious behaviour.\(^3\) Employees “can initiate great harm to the confidentiality, integrity, or availability of information security through deliberate activities (disgruntled employee or espionage) or they may introduce risk via passive non-compliance with security policies, laziness, sloppiness, poor training, or lack of motivation to vigorously protect the integrity and privacy of the sensitive information of the organisation and its partners, clients, customers, and others.”\(^4\).

Given the potential threats for the value attached to information resources, companies are increasing their efforts to counteract these risks, introduced by employees. With this in mind, it is no surprise that many company security technologies are strongly focused on analysing employee behaviour in order to detect and prevent incidents. An example of such a monitoring tool is MUSES (Multiplatform Usable Endpoint Security)\(^5\). MUSES is a user-centric security system that aims to enhance company security by reducing security risks introduced by user behaviour. However, even though the monitoring of employees may be beneficial for the information security of the company, monitoring of employees is restricted by privacy and data protection law.

In this paper, we use the MUSES Real-Time Risk and Trust Analysis Engine (MUSES RT2AE) as a use case to study in which way privacy and data protection legislation restricts the monitoring of

---

\(^1\) Note that the notion of insider covers a broader scope of actors than only employees. Definition of insider: “An ‘insider’ is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organisation’s structure”, by C.W. PROBST, J. HUNKER, D. GOLLMANN, and M. BISHOP, Insider Threats in Cyber Security, New York, Springer, 2010, 5.


\(^5\) MUSES (Multiplatform Usable Endpoint Security) project, funded by the EU IST Seventh Framework Programme under the grant agreement number 318508, see: https://www.musesproject.eu/.
employees via company security technologies. In Section 2 we present the studied MUSES RT2AE component as part of the MUSES system. In section 3 we analyse the legal requirements following from EU privacy and data protection law applied to the employment context. In section 4 we clarify why security technologies face difficulties in aligning privacy and security interests, and how this discrepancy may be neutralised. In section 5 we discuss how the design-process of the MUSES RT2AE was influenced by privacy and data protection requirements, without neglecting the main security purpose of the system. Finally, in Section 6, we conclude our findings.

2. TECHNICAL BACKGROUND: THE MUSES RT2AE COMPONENT

The MUSES RT2AE was developed in the MUSES project.\textsuperscript{6}

In general, MUSES (Multiplatform Usable Endpoint Security) aims to enhance corporate security by reducing security risks introduced by user behaviour. The core idea of MUSES is to highly secure cloud based company data assets through a device independent user-centric and self-adaptive corporate security system. MUSES is able to cope with the concept of seamless working experience on different devices, meaning that a user may start a session on a device and location and follow up the process on different devices and locations, without corporate digital asset loss.

The overall MUSES architecture includes a number of tools and mechanisms for user-friendly and secure human interaction over multiple devices.\textsuperscript{7} One key element is the RT2AE (Real-Time Risk and Trust Analysis Engine), which is a component in the Continuous Real-Time Event Processor (MusCRTEP) in MUSES.\textsuperscript{8} One of the design goals of the RT2AE was to be adaptable to enable different types of risk and trust metrics at a later stage, without too many changes to the component itself. Thus, to make it possible to integrate metrics that have been developed outside of MUSES, e.g., metrics with improved attack-resistance. The RT2AE aims to prevent or at least reduce potential data loss damage by allowing or denying access to company assets based on the Trust-Value of the user and his computing device environment.\textsuperscript{9} To this end, the RT2AE compares the potential value for the company by allowing access to an asset under certain conditions, with the potential risks that might be brought by the access.\textsuperscript{10} This means that even if the data get lost or compromised after access is allowed, the potential added value for the company, by allowing access, is still higher than the estimated damage.

In order to allow the RT2AE to perform an accurate risk analysis, the engine analyses several contextual elements relating to the user/employee and the device being used to request access.\textsuperscript{11} First, the RT2AE requests the location of the user, in order to know whether the employee is inside or

\textsuperscript{6} MUSES (Multiplatform Usable Endpoint Security) project, funded by the EU IST Seventh Framework Programme under the grant agreement number 318508, see: https://www.musesproject.eu/.
\textsuperscript{8} J.-M. Seigneur, C. Ballester Lafuente, X. Tití, and J. Guislain, Revised MUSES trust and risk metrics, MUSES project, D3.3, 2014, 8.
outside the company buildings or in any other safe area. Secondly, the RT2AE analyses the connection by which the company asset is requested in order to assess the reliability of the network at the moment of request. To this end, the RT2AE makes a distinction between secure connections, for example when an employee requests access using his home network, and unsecure connections for when the employee requests the access via a public wifi network. Thirdly, the RT2AE could be enabled to have access to the professional calendar of the employee in order to know the timeframe in which an employee is assigned to work on the requested asset. Fourthly, the RT2AE also includes the wage of the employee in the assessment of the Risk Opportunity Benefit. Fifthly, the RT2AE uses the previously calculated User Trust-Value of an employee. This User Trust-Value is a user-specific value which represents the user’s level of trustfulness. Although all users start with the same value, this value might change over time depending on previous incidents or breaches.

Moreover, the RT2AE also requires company-related information. A first contextual factor relates to the cost of the company asset. The CSO is charged with the task of pointing out the value of each category of assets. A second parameter relates to the status of the asset. This status shows whether the requested asset has been reviewed by the CSO or an IT security expert and if so, whether it was flagged as compromised or security incident free. Moreover, the RT2AE analyses the company security policies and the risk policies at the time of the request. This is necessary as the rules set out by the company regarding access could be overruled by the benefit access could bring to the company given the exceptional circumstances of the request.

The information described above is used by MUSES to determine whether a user has the right and/or ability to usefully access company assets. Comparing the potential damage introduced by the location of the user, the type of internet connection being used for the access, the time the employee may work on the asset, etc. with the risk of losing the asset, according to the values set by the CSO, the RT2AE estimates the risk the access may bring. If the asset is flagged as security free and the employee is, according to the company policies, authorised to access the requested asset, MUSES grants the user access. However, even if the RT2AE concludes that certain risks could compromise the security of the company, access may still be granted if the Risk Policy analysis indicates the higher benefit for the company to allow the user access to the requested asset.

In case of denied access, MUSES informs the employee about the denial and the reasons on which this decision was based.\textsuperscript{12}

3. LEGAL BACKGROUND: P/DP IN THE WORKPLACE

The right of the company to protect company assets and to monitor and control employees has to be balanced with the privacy and data protection rights of the workers. The right of the employer to exercise his right to authority shall thus be restricted in accordance with the applicable legal framework on privacy and data protection.

3.1 PROTECTION OF THE PRIVATE LIFE OF EMPLOYEES

The right to respect for privacy is an internationally recognised fundamental right. As an established core value of the democratic society, it is (at least implicitly) recognised in all major international

treaties on human rights, such as Article 7 of the EU Charter and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention), as well as in almost all national constitutions.\textsuperscript{13}

Already in 1950 the Council of Europe enshrined the right to respect for private life and family life in Article 8 of the European Convention.

In order to avoid that too many intrusions would be excluded from the scope of Article 8 of the European Convention, the European Court of Human rights interprets the notion of private life very broadly.\textsuperscript{14} According to the Court, the provision also applies in public spaces. It found that “there might be a zone of interaction of a person with others, even in a public space, which may fall within the scope of ‘private life’\textsuperscript{15}. Such private life can also be found in the workplace.

In the Niemietz case the Court held that “virtually all professional and business activities may involve, to a greater or lesser degree, matters that are confidential\textsuperscript{16} and that “respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of ‘private life’ should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world\textsuperscript{17}.

In the Halford case, the Court held the opinion that the interception of a worker’s telephone calls at work may violate her right to respect for private life. In this case, Ms Halford had invoked a breach to her right to privacy, as the British police, her employer, had intercepted her home and office telephone calls to gather evidence against Ms Halford, to use in an earlier discrimination case. The Court rejected the statement of the British government that “calls made by Ms Halford from her workplace feel outside the protection of Article 8, because she could have had no reasonable expectation of privacy in relation to them”\textsuperscript{18}. According to the Court this argument was invalid, since “it is clear from its case law that telephone calls made from business premises as well as from the home may be covered by notions of ‘private life’ and ‘correspondence’ within the meaning of Article 8, (1)\textsuperscript{19}. All correspondence from the workplace falls within the scope of Article 8 of the European Convention.

In the Copland case, the Court confirmed its earlier opinion on the wide scope of Article 8 of the European Convention in the workplace. Not only paper letters and telephone calls are protected by Article 8. In the Copland case, the Court broadened the scope of communicational privacy protection to also include the Internet use of workers and the electronic communication of workers, such as e-


\textsuperscript{14} For example, see: ECtHR 22 October 1981, No. 7525/76, Dudgeon v. the United Kingdom; ECtHR 15 May 1992, No. 15666/89, Kerkhoven and Hinke v. the Netherlands; ECtHR 16 December 1992, No. 13710/88, Niemietz v. Germany; ECtHR 25 March 1993, No. 13134/87, Costello-Roberts v. the United Kingdom; ECtHR 25 June 1997, No. 20605/92, Halford v. the United Kingdom.

\textsuperscript{15} ECtHR 25 December 2001, No. 44787/98, P.G. and J.H. v. the United Kingdom, §56; ECtHR 28 April 2003, No. 44647/98, Peck v. the United Kingdom, §57.


\textsuperscript{17} ECtHR 16 December 1992, No. 13710/88, Niemietz v. Germany, §29.

\textsuperscript{18} ECtHR 25 June 1997, No. 20605/92, Halford v. the United Kingdom, §43.

\textsuperscript{19} ECtHR 25 June 1997, No. 20605/92, Halford v. the United Kingdom, §44.
mails and related files attached thereto. The Court held that it is only logical that “e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage”\textsuperscript{20}. The Court observed that “the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an integral element of the communications made by telephone”\textsuperscript{21}. Accordingly the Court considered that “the collection and storage of personal information relating to the applicant’s telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8”\textsuperscript{22}.

3.2 PROTECTION OF THE PERSONAL DATA OF EMPLOYEES

3.2.1 WIDE ARRAY OF DATA PROTECTION LEGISLATION

As information technology advanced, the awareness of data privacy grew with it. In our current information society, ‘informational privacy’ refers to the protection of persons from “privacy invasions that occur as a result of the use and disclosure of personal information gathered and stored in computerized databases, often gleaned from the Internet”\textsuperscript{23}.

To meet the needs of the changing society the Council of Europe adopted a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981.\textsuperscript{24} In 1989, a Recommendation on the Protection of Personal Data used for Employment purposes, expanded this Convention to the workplace context.\textsuperscript{25}

Within the European Union the significance of informational privacy was explicitly recognised in Article 8 of the European Charter of Fundamental Rights of the European Union\textsuperscript{26}, by which it was elevated to a fundamental status. The EU Charter, binding on the EU Member States, also provides for a European fundamental right to respect for private life in Article 7, which is similar to the one in the European Convention.

As a result of Article 16 of the Treaty on the Functioning of the European Union which enables the European Parliament and the Council to “lay down the rules relating to the protection of individuals with regard to the processing of personal data”, two essential EU Directives were adopted.

First, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of

\textsuperscript{20} ECtHR 3 April 2007, No. 62617/00, Copland v. the United Kingdom, §41.
\textsuperscript{21} ECtHR 3 April 2007, No. 62617/00, Copland v. the United Kingdom, §43.
\textsuperscript{22} ECtHR 3 April 2007, No. 62617/00, Copland v. the United Kingdom, §44.
such data (hereafter referred to as Directive 95/46/EC or the Directive)\textsuperscript{27}, which is the cornerstone of EU data protection.


In particular with regard to the employment context, also several non-binding legal instruments are to be pointed out. First, there is Recommendation No. 89 2 on the Protection of Personal Data used for Employment Purposes, which was adopted by the Council of Europe in 1989.\textsuperscript{29} Further, there are the ILO Guidelines on the Protection of Workers’ Personal Data from 1997.\textsuperscript{30} And finally, on the level of the European Union level, relevant are the opinions and working documents adopted by the Article 29 Data Protection Working Party. With regard to the employment context, the Working Party issued two interesting documents, being Opinion 8/2001 on the processing of personal data in the employment context\textsuperscript{31} and the Working Document on the surveillance of electronic communications in the workplace.\textsuperscript{32}

3.2.2 EU DIRECTIVE 95/46/EC

Without any doubt, Directive 95/46/EC is still the reference text on the protection of personal data in the European Union. Even though the legal framework on data protection is currently under reform.\textsuperscript{33} In this paper the analysis of the future, currently only proposed, legislation is limited to stress or distress the key notions of our research.

Although Directive 95/46/EC does not explicitly mention the monitoring of workers, the Article 29 Working Party stated repeatedly that the EU data protection requirements, following from the this Directive, also fully apply in this field.\textsuperscript{34}


\textsuperscript{34} Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 4: "Data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, Internet access, video cameras or location data. Any monitoring must be a proportionate response by an employer to the risk it faces taking into account the legitimate privacy and other interests of workers. Any personal data held or used in the course of monitoring must be adequate, relevant and not excessive for the purpose for which the monitoring is justified. Any monitoring must be carried out in the least intrusive way possible", http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf; Article 29 Working Party, Working...
3.2.2.1 **NOTION ‘PERSONAL DATA’ AND ‘PROCESSING OF PERSONAL DATA’**

Directive 95/46/EC protects data subjects whose personal data are processed. According to Article 2, a) of the Directive, personal data is “any information relating to an identified or identifiable natural person (‘data subject’)

The notion of ‘processing of personal data’ is defined in Article 2, b) of Directive 95/46/EC, as: “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”. This is a widely formulated definition including basically all operations one could possibly perform upon personal data. Hence, the processing of personal data is not limited to automated processing operations. However, in order to fall under the protective scope of Directive 95/46/EC, for manual processing it is required that the processing forms a part of a filing system (Art. 3, 1) Directive 95/46/EC). Also outside the scope of the Directive are the processing of personal data which concerns “public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law” (Article 3, (2), first sentence DP Directive), and the processing operations “by a natural person in the course of a purely personal or household activity” (Art. 4, 2), second sentence Directive 95/46/EC).

3.2.2.2 **FORMAL REQUIREMENT TO RESPECT THE LAW**

Directive 95/46/EC sets out a list of requirements for the processing of personal data. Article 6, 1), (a) requires that the processed data must be ‘processed fairly and lawfully’, meaning that the personal data “must be processed in a way that does not bring about a breach of either data protection law or other legal requirements”\(^{35}\), either general or specific for workers.

With regard to the protection of personal data of workers, it should thus be noted that data protection law does not operate in isolation from labour and employment law and practice, nor does labour and employment law and practice operate in isolation from data protection law. The Working Party points out that this is as a necessary and valuable interaction, as it should assist the development of solutions that properly protect the interests of workers.\(^{36}\)

The regulation on the protection of workers is regulated through several international treaties, codes and practices, by the Council of Europe and the European Union. Furthermore, the creation of labour and employment law continuous on national level, sectorial level and company level. Due to the excessive amount of labour and employment legislation and different policy-makers in the EU Member States, a comprehensive overview of those would largely exceed the scope of this paper. However, it must be mentioned that in any case, the conditions under which monitoring of workers is allowed in a company, have to be defined and specified further on company level. In order to legally monitor worker behaviour, the company must carefully include strict and clear procedures within its company policies on Internet use, security, BYOD or any other policy.


3.2.2.3 Legal Ground for the Processing of Personal Data
Moreover, Article 7 of the Directive 95/46/EC sets out the substantive criteria for the legitimate processing of personal data. In order to legally process the personal data of workers, the processing must be based on at least one of the legal grounds as laid down in Article 7 of the Directive.

The most likely relevant legal grounds for the processing of personal data in an employment context are those where the processing is necessary for the performance of a contract, when it is necessary to comply with a legal obligation, or when it is necessary to protect the legitimate interests of others.

A specific difficulty rises with regard to the employee consent, referred to in Article 7, (a) and Article 8, 2), (a) of the Directive. Where there is a clear imbalance between the data subject and the controller, consent should not provide a valid legal ground for the processing of personal data. It is widely accepted that the free nature of a consent may be a problem in a professional context due to the existence of a relationship of subordination. The Article 29 Working Party “takes the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent”37. Reliance on consent should therefore be “confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment”38. The imbalance between employer and employee was also explicitly recognised as an obstacle for employee consent in the first proposed Data Protection Regulation. However, in later versions the explicit reference was removed.39

The legal grounds for the processing of personal data must always be interpreted in relation to the applicable national law. For example, Article 5 of the Belgian Collective Bargaining Agreement No. 81 on the monitoring of employees allows employers to monitor the electronic communication of employees if the monitoring is aimed to the security and/or the adequate technical functioning of the IT-network systems of the company or for the protection of sensitive economical, trading or financial interests of the company.

3.2.2.4 Substantive Requirements for the Processing of Personal Data
Further, Article 6, 1), (b) of Directive 95/46/EC requires that personal data may only be collected for specified, explicit and legitimate purposes and that personal data shall not be processed in a way incompatible with those purposes. In terms of data protection principles, this principle is called the principle on purpose specification and limitation.

In 2013, the Article 29 Working Party adopted an opinion on purpose limitation.40 According to this opinion, the purpose limitation principle protects data subjects by setting on how data controllers are able to use their data while also offering some degree of flexibility for data controllers. The Article 29 Working Party divides the principle in two main building blocks: first, personal data must be collected for ‘specified, explicit and legitimate’ purposes (purpose specification), and second, these data must

not be ‘further processed in a way incompatible’ with those purposes (compatible use)’\textsuperscript{41}. The principle of purpose specification implies that the personal data are collected for certain aims, the ‘raison d’être’ of the processing operations. From the principle of purpose limitation it follows that personal data cannot be further processed when such an operation would be incompatible with the initially specified purposes. As a result thereof, the processing of personal data must always be compatible with the defined purposes.

Even when the processing of personal data is specified for a legitimate purpose, the processing operations must still comply with the requirement of necessity. This means that the processing of personal data only takes place when it is ‘necessary for’ the “achievement of the objective in question rather than merely incidental to its achievement”\textsuperscript{42}. Personal data can only be processed when this is adequate, relevant and not excessive in relation to the specific purpose for which the data were collected. Hence, the processing of personal data has to be carried out in the least-intrusive way, considering, e.g. the risks at stake, the amount of data involved, and the purpose of processing.

This implies that employers should always process the personal data of workers in the least-intrusive way. To this end, different elements should be considered. The least intrusive way depends for example on

Another aspect of data quality is the obligation to process accurate and kept up to date data as laid down in Article 6, 1), (d) of Directive 95/46/EC.

According to the Article 29 Working Party employers are obliged to “take every reasonable step to ensure that data are not inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, erased or rectified”\textsuperscript{43}.

The last data quality principle relates to the retention of personal data. From Article 6, 1), (e) of Directive 95/46/EC it follows that records on worker behaviour “must be kept in a form which permits identification of workers for no longer than is necessary for the purposes for which the data were collected or for which they are further processed”\textsuperscript{44}.

3.2.2.5 Rights of the Data Subject

Article 10 and 11 of Directive 95/46/EC provide data subjects with the right to information. Whenever personal data of an individual are processed, the individual must be informed about the data that will be processed about him, and about the consequences of the processing.

Moreover, data subjects are provided with the right to access. This right also covers the right to rectification, erasure and/or blocking of data which processing does not comply with the Directive (Art. 12 Directive 95/46/EC).

The third right of the data subject is the right to object against wrongful processing or against the processing of his personal data for direct marketing purposes (Art. 14 Directive 95/46/EC).

\textsuperscript{41} Article 29 Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP203, 3.
Moreover, data subjects have the right to judicial remedy in case of breach (Art. 22 Directive 95/46/EC).

Finally, Article 15 of Directive 95/46/EC protects data subjects against automated individual decisions. An automated individual decision is a decision that significantly affects a person and which is based solely on automated processing of personal data in order to evaluate him as a person. Since such an evaluation may relate to different personal aspects, such as performance at work, creditworthiness, and reliability, the decisions made by the MUSES system should be considered as automated individual decisions. Automated individual decisions are in principle prohibited, although, this prohibition does not apply when the decision is taken in the context of an agreement, which also lays down measures to safeguard the data subject’s legitimate interests (such as objection to wrongful decisions). Yet again, the information and transparency towards the data subject are an essential condition for legitimate processing of personal data. This provision receives special attention in the proposed Data Protection Regulation, where it is included in Article 20 ‘Measures based on Profiling’. The proposed Regulation considerably enlarges the protection in respect of automated individual decisions in relation to profiling, which will cover also the use of data correlations to predict behaviour, or to take decisions vis-à-vis targeted people. The proposed provision protects data subjects against measures that produce legal effects for them or significantly affects them, when these measures are based solely on automated processing, intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person’s performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

3.2.2.6 Obligation to take security measures

Article 17, 1) of Directive 95/46/EC obliges the data controller to take security measures. The employer must implement appropriate technical and organisational measures in the workplace, in order to safely secure the personal data of his workers from outside intrusion. Personal data must remain safe from the curiosity of other workers and/or third parties. Hence, this security principle also encompasses a ground for the employer to protect the company networks against intrusions and attacks.

4. Difficulties regarding privacy and data protection in security technologies

Security technologies require huge amounts of information, including personal data. As set out in Section 2, the MUSES RT2AE requires contextual information about the user and the user’s device to calculate whether or not access to company assets can be granted. This information may include personal data, such as the location of the user. From Section 3 it is clear that whenever personal data about the user are processed, data protection law must be complied with.

The tension between the necessity for security technologies to collect information and the restrictions following from privacy and data protection law lead to the idea that privacy and security are hard to align.

4.1 Legal Position of the Developer

The responsibility to comply with the law for the processing of personal data, and hence, the monitoring, remains with the data controller, the company.

EU law appoints the data controller as the responsible person in data processing operations. The controller is the natural or legal person who determines the purposes and means of the processing of the personal data (Article 2, d)-e) Directive 95/46/EC). Directive 96/46/EC also foresees in the role of processor, for whom the processing of data is determined by the controller.46

A developer is neither a controller nor a processor. Hence, there is currently no obligation (yet) for developers to design their systems in the most privacy-friendly way. Moreover, given that the goal of a security technology is to secure company assets, and those technologies are developed to serve and to be purchased by companies, privacy and data protection are often out shadowed by the company’s security interests.

4.2 Privacy and Data Protection by Design

However, given the rapid nature and the complexity by which communication technologies has advanced, it became increasingly apparent that privacy had to become the default mode of design and operation.47 Privacy by design meets this new need as it is an approach to “protect privacy by embedding it into the design specifications of information technologies, accountable business practices, and network infrastructures, right from the outset”48.

The idea of privacy by design is to integrate privacy-requirements and privacy-preserving solutions in the engineering of products and services (privacy engineering). As such, privacy becomes an essential component in the core of the delivered functionality. Privacy becomes an integral part of the system without diminishing functionality.49 In other words, in order to mitigate privacy concerns and to achieve data protection compliance50, privacy should be embraced from within the systems.

In Europe, the "momentum behind privacy by design has been steadily growing. It is increasingly becoming a 'basic principle' of data protection"51. Already in 2009, the Article 29 Working Party and the Working Party on Police and Justice issued a joint opinion advocating for the incorporation of the principles of privacy by design into a new EU privacy framework.52 Later in March 2010, the European Data Protection Supervisor followed this opinion in a recommendation recommending to “include unequivocally and explicitly the principle of privacy by design into the existing data protection

49 A. CAVOUKIAN, Privacy by design: the 7 foundational principles, Information and privacy commissioner of Ontario, Canada, 2009.
regulatory framework.” The European Commission took these recommendations into account in the data protection reform package and the notion of privacy (currently data protection) by design was formally introduced into the core of the European Union’s data protection law in Article 23 of the proposed EU Data Protection Regulation (2012).

Since 2012 the text of Article 23 has been subject to many changes. Currently, Articles 23 of the Proposal is stated as follows:

“Having regard to available technology and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (...) technical and organisational measures appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation, in such a way that the processing will meet the requirements of this Regulation and protect the rights of (...) data subjects.

The controller shall implement appropriate measures for ensuring that, by default, only (...) personal data (...) which are necessary for each specific purpose of the processing are processed; this applies to the amount of (...) data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.”

Once the General Data Protection Regulation enters into force, the theory of privacy by design shall have an enforceable ground within Europe.

4.3 PRIVACY AND DATA PROTECTION AS AN ADVANTAGE FOR DEVELOPERS

Without delving into the procedural burdens of enforcing privacy at later stages, it may be emphasised that privacy is at risk, as the security interests of companies will not align better with the privacy-friendly business interests of security technology developers, and the lacking liability for designing privacy-unfriendly tools and systems remains unsanctioned. The question is how technology can meet privacy and data protection requirements, even before the proposed General Data Protection Regulation enters into force.

Indeed, even though there is no responsibility for developers, there is still a business advantage to it. As Wojciech Wiewiórowski, Assistant European Data Protection Supervisor, emphasised: “Privacy and data protection are not barriers to economic growth and international trade, rather they enhance them. Trust is a necessary precondition for innovative products and services that rely on the processing of personal data. The EU’s aim to grow the digital single market will be successful but only

---

53 European Data Protection Supervisor, Opinion of promoting trust in the information society by fostering data protection and privacy, adopted on 18 March 2010, 8.
if the interests of the individual are protected. A new deal for citizens’ rights can galvanise responsible businesses and public authorities.\textsuperscript{56}

5. Privacy and Data Protection in the MUSES RT2AE

MUSES was developed with the user at heart. For this reason, technical enhancements were made to embed privacy and data protection in the MUSES design.

5.1 Four Key Guidelines during the Development of MUSES

In order to facilitate companies to make privacy-friendly choices, the MUSES system was developed with four key principles in mind: the principle of purpose limitation, data minimisation, security and transparency.

Based on those four key principles, and with the privacy by design principles\textsuperscript{57} in mind, four guidelines were drafted to support the developers of the MUSES system.

<table>
<thead>
<tr>
<th>Principle</th>
<th>MUSES guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose limitation</td>
<td>Describe for all components in the system the core purposes served and the main functions delivered (e.g., company information security). Include privacy as a goal, and provide the highest degree of privacy protection for personal information possible while serving the core purposes of MUSES and delivering the other main functions of the system.</td>
</tr>
<tr>
<td>Data minimisation</td>
<td>Incorporate data minimisation by anonymisation and pseudonymisation, decentralised storage of personal information, dynamical data retention assessments, etc. Whenever reasonably possible, provide data protection as a default setting: automatically without any actions by individual users is required to protect their personal information.</td>
</tr>
<tr>
<td>Data security</td>
<td>Employ the maximum feasible means needed to ensure the security, confidentiality, and integrity of personal information throughout the lifecycle of the data (by e.g., encryption and shielding of data).</td>
</tr>
<tr>
<td>Transparency</td>
<td>Ensure that the system informs the users about the collection and processing of their data, the further use, disclosure, etc. before the data are collected. Ensure that the system informs the users about its decisions and the reasons behind denials. In addition, ensure that the system remains reasonably transparent and subject to independent verification.</td>
</tr>
</tbody>
</table>

Table 1. Guidelines for developers


\textsuperscript{57} Based on: A. CAVOUKIAN, Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers, Information and privacy commissioner of Ontario, Canada, 2011.
5.2 Applied to the Four Stages of the Data Lifecycle in MUSES

In the consideration of the four key guidelines, the MUSES developers made a distinction between four stages in the lifecycle of the data. These stages refer to the collection of the data, the storage of the data, the processing of the data and the final erasure of the data.

For the MUSES RT2AE the data lifecycle can be illustrated as follows: when an employee requests access to a company asset, the MUSES RT2AE retrieves contextual information collected by the sensors, in order to assess whether or not access can be granted. The decision of the MUSES RT2AE is stored in the MUSES database. Once the information is no longer deemed to be necessary, this information is erased from the database.

Several MUSES design-decisions were influenced by the four key data principles set out here above. As one type of Trust-Values in the MUSES RT2AE strongly relates to the trustworthiness of the user, the key guidelines particularly influenced the RT2AE design. Below we discuss for each stage a few examples that relate to the decisions made by the RT2AE.

5.2.1 Data Collection

Imagine a company security policy that allows access to file-type X only when the user is inside the company premises or at home. In order for MUSES to acquire the information about the user’s location, it could use the GPS-function on the mobile device, the Wi-Fi connection, maybe a cell tower for coarse location or a combination of those options. However, the location of users is considered as personal information. In respect of the data minimisation principle the MUSES was designed to not store data about the user’s location in terms of longitude and latitude, but to define a zone and check whether the user is within the specified zone or not.

After the user and device information is collected, the user’s device communicates this information to the MUSES server in order to allow the RT2AE to grant or deny access to a company asset. The communication between the device of the user and the server is encrypted.

5.2.2 Data Storage

All information necessary for the MUSES processing operations is stored in a central MUSES database.

Since the protection provided by Directive 95/46/EC only concerns the processing of personal data, anonymised data fall outside of the scope of the protection. However, in this regard, the concept of pseudonymisation should be mentioned. Article 4, 3b of the proposed General Data Protection Regulation defines pseudonymisation as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational

measures to ensure non-attribution to an identified or identifiable person” 62. Hence, pseudonymisation can be seen as the technical process of disguising identities. In this process personal identifiers are replaced in a dataset with other values (pseudonyms). Such a dataset makes it possible to collect data relating to the same individual, without having to know his or her identity. However, retraceable pseudonymised data may be considered as indirectly identifiable personal data if it is still possible to backtrack to the individual 63. Nevertheless, can “the application of pseudonymisation to personal data [...] reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations” 64. For this reason, MUSES stores the information about a user in a pseudonymised format, in which the identity of the user is revealed, while still allowing the system to link related incidents to the same user.

The MUSES database stores the data divided in different categories. The access to this information by the different MUSES components can only be enabled in the design of the requesting component. Hence, not all components may have access to the same categories of data in the MUSES database (limited access to the stored data).

In addition, also the security principle influenced the manner in which information is stored in MUSES. For example, in case no secure connection with the MUSES server could be established, information is temporarily saved in an isolated storage space on the user’s device. Only after the device establishes a secure connection with the server, these data are send to the server and erased from the isolated local space.

5.2.3 Data erasure

MUSES does not keep data longer than necessary. In order to facilitate the erasure of abundant information, a privacy enhancing system, called the MUSES Privacy Shield, was developed to follow up the interactions between the components and the database. Within the storage limitation a distinction was made between hard and soft limits.

The MUSES Privacy Shield first assesses whether no hard limits for storage are approaching. Hard limits are based on the law, for example, when a specific national law foresees in a maximum retention period of monitoring logs. Therefore, MUSES facilitates the technical means for the CSO to set different time limits for the different categories of the data, depending on company-specific legal restrictions. Moreover, the MUSES Privacy Shield allows MUSES to easily erase the datasets relating to a certain employee, for example, when he is no longer employed by the company. In this regard it could be pointed out that this could be achieved even automatically. Given that the wage of employees is an essential parameter in the MUSES RT2AE analysis and that this information could be retrieved via payroll information, then, the data about a user could be erased once MUSES detects the absence of payroll activity to a certain employee for a certain time.

On the other hand, there are soft limits. Those limits depend on the necessity and accuracy of the personal information in relation to the purposes of the different MUSES components and will be automatically-dynamically assessed by the MUSES Privacy Shield. For example, while the MUSES

---

RT2AE requires the User Trust-Value in order to grant the user access to a company asset, it only requests the last User Trust-Value, as the previous User Trust-Values are implicitly included in the value of the last one.

5.2.4 Data analysis

The MUSES RT2AE could have used e-reputation, extracted from social media information, as a variable to calculate the risk. However, after analysing the risks aspects of the IT security application domain,\(^65\) it was opted to use the User Trust-Value only to fine tune the risk analysis. Other risks were found to be much more important for the risk decision-making than the User Trust-Value. For example, if the network is currently under attack, the fact that a user is more or less trustworthy becomes moot. Thus, given the privacy risks that e-reputation retrieved from social network information would create, compared to the low utility of the extra processed user information, the research on e-reputation information was not pursued further and hence not included in the design of the MUSES RT2AE.

For the same reason, also the previous user data were excluded from the RT2AE analysis. Instead of requesting all previous User Trust Values in case a SecurityIncident occurs, the MUSES RT2AE now only requests an update from the last User Trust Value.

6. Conclusion

Successful protection of company data assets requires strong technological support. As many security incidents still occur from within, security technologies often include elements to monitor the behaviour of employees. As those security systems are considered as privacy-intrusive, they are hard to align with the privacy and data protection rights of the employees of the company.

Even though there is currently no legal obligation for developers to embed privacy and data protection in security systems, by taking privacy-friendly design decisions, developers can play a significant role in the protection of employees.\(^66\) Especially since privacy by design is gaining momentum in Europe, but nonetheless, because privacy and data protection law results in several obligations for companies, and the non-compliance with data protection law is increasingly under fire, the need for companies to deploy privacy-friendly security systems, is growing. Hence, developers will also increasingly benefit from designing privacy-friendly security systems.

In this paper the MUSES RT2AE was studied as an example of privacy-friendly development of a security system. The MUSES developers used four privacy and data protection guidelines in order to make privacy-friendly design choices. Besides several limitations on the type of information which is processed by MUSES, MUSES technically facilitates companies to modify the privacy-friendliness of the system according to the specific needs of the company. Nevertheless, the road to privacy-friendly security technologies is long and hard to pave, but step by step, all of us will get there.

7. ACKNOWLEDGMENTS

The research leading to these results has received funding from the EU IST Seventh Framework Programme (FP7) under the grant agreement number 318508, project MUSES (Multiplatform Usable Endpoint Security).