Linnaeus University, Dept. of Informatics
Lars Magnusson (lm222mc)

Building Activist and Public Services without Compromising EU-GDPR

Lars Magnusson, M.Sc. CISSP ITIL

Paper

5IK502 - Contemporary issues in IS research and development
Jan 10, 2017

Introduction

Internet has during the last 15 years become an integral part of our lives and together with tools like smart-phones and tablets profoundly changed the world to its roots. Doesn't matter where you are, in Africa, the island world of the Pacific, the Arctics, even the Antarctic or on a plane or ship out in the middle of an ocean, you have Internet with you.

Internet is no longer the tool of the affluent, it is the tool for everybody, even if you still is a "head hunter" in Papua New Guinea. In the early 2000:s there was a cartoon circulating, two white explorers sitting at a camp fire in the jungle, a cannibal visiting them, asking if he could check his Facebook account. Well, today he likely communicates via his own smart-phone, powered by a solar panel.

Today we cannot envision a world without mobile devices and Internet. Still, it is a technology with only 30-35 years history, evolved over a single generation. People living their lives, not too far from the film "Matrix". An opportunity for both the users, as the society. But remember George Orwell's "1984".

For this author, being a part of this revolution since 1966, it is a blessing and a curse. Being a dyscalculic, the calculators of late 1960:ies and the programmable ones in the 1970:ies was a blessing. Still, as an Information Security Professional, I daily see the drawbacks.

In the same way, smart-phones have been the same blessing for people in socially weak positions or engaged in public activism. Giving these groups control over their own life (Pendse, 2015), like me with my calculators. Taking control over your situation, bending the negative to something positive. Homeless able to interface with their personal as professional support networks. Christopher Le Dantec at Georgia Tech (Le Dantec, 2008; Le Dantec et.al., 2011; Asad and Le Dantec, 2015) have done a large number of studies how these tools give marginal groups a sense of self-respect and the ability to better address their problems.

But also as targets for non-democratic or even criminal take-overs. In 2014 we saw a substantial shift in the international IT market's view regarding information security. A shift to a very bleak outlook, where, as an example, a Symantec representative declared: "Anti-virus is dead" (Chacos, 2014; Whittaker, 2014). Though a bit to defeatist, he tried to point out what the joint Internet information security community daily experiences; that the "Bad Guys" is getting better than the "Good Guys" (WEF, 2014). More professional and with better resources, they able to mounts attacks far more successful than only some years back.

As discussed in media and at many events, the current time for a security breach is about 5 hours, while average time of discovery is over 200 days (Hart, 2015; Hansen, 2015). To wreak havoc, maybe using the time to via the victim, breach other victims (Hardekopf, 2015). There always will be flaws, as stated by "Murphy's Law" (Murphy, 1949).

As a result of this status, Europe instigated a new 2018 EU data privacy framework, EU General Data Protection Regulation (EU-GDPR or GDPR) (EU (1), 2016), having a formidable impact on all this. "Keep Data Save" and "Secure by Design", two hard concepts that can cost the "Data Controller", i.e. the one handling data, up to some 4% of the total global turnover or if less than €20M, up to that. GDPR would be the death to these services, but do it need to?

This paper is to look at such non-commercial mobility networks, discussing them in the context of social impact, as well as out of security and mainly EU-GDPR. The paper also touch some architectural possibilities, maybe solving the issues for these networks when adhering to GDPR.

1. Problem Introduction

> "A man that sets out to justify his existence and his activities has to distinguish two different questions. The first is whether the work which he does is worth doing; and the second is why he does it, whatever its value may be"
> (D.H. Hardy, 1940, "A Mathematician's Apology")

As mentioned in the introduction, we have economically weak groups increasingly engaged in using modern mobile technology, to support society-wise very beneficiary initiatives. Like Hardy said in 1940, they think it's worth the effort and something needs doing.

There has been a sizeable discussion about ethnography as a tool in developing new efficient ITC system solutions. As shown by Le Dantec et al (Le Dantec, 2008; Le Dantec et.al, 2011; Asad and Le Dantec, 2015) the public sector, including civil activism, do benefit of the usage of modern mobile solutions. They improve life for the participants in substantial ways.

The key is that many today socially disadvantaged individuals do have access to cheap mobile phones, even smart-phones (Le Dantec, 2008; Le Dantec et.al, 2011; Asad and Le Dantec, 2015; Pendse, 2015, UN, 2015). After the turn of the century we have seen a substantial increase in connectivity. Both in 3:d world countries (Bank, 2013; Balch, 2014; Pendse, 2015; UN, 2015), as among poor people in the industrialised world. Much credited to the cash cards (Pendse, 2015), available for a low cost from most telecom companies. These cell phones is mostly used for the cheaper sms messages or using an included Internet pot (Le Dantec, 2008; Le Dantec et.al, 2011; Asad and Le Dantec, 2015, Pendse, 2015). Thus giving previously marginalised groups a working access to the "normal" world, without giving up their privacy or predicaments.

However, being low key development efforts, with less funding than commercial applications grazing the same turf, like Uber, AirBnB etc; since these applications do handle sensitive data about the users, so particular within the European Union, we end up in a discussion about data protection.

A discussion that has become greatly intensified with the April 2016 EU Parliament ratification of the May 25, 2018 EU General Data Protection Regulation [EU-GDPR or simply GDPR] (EU (1), 2016). With its currently theoretical extensive fines, it suddenly put a substantial responsibility on those developing this type of applications (EU (2), 2016). Independent if it is civil activists or public support projects.

The intention of this paper is to look at the future of this type of activism/public service due to this development.

The initial intention was to use a Swedish case, reviewing their thoughts and intentions. However, after discussing the issue with the country's largest activism support group, "Youth Media" (ungmedia.se, personal communication, 2016), supporting some 100 organizations and 5.000 media oriented activist members, unfortunately this type of "hacktivism" proved to be too much in it's infancy to draw any conclusions. Their understanding of the aspects of security and particular GDPR was very limited. So limited, that they could not be used as a test case.

This author therefore reverted to review one of Le Dantec's cases (Le Dantec et.al, 2011). Albeit a US case, but still a plausible one for possible future European digital social services. The case chosen was a case of marginalised single, sometime drug using, mothers. The intention was to help them with general support, health care and their children's school

planning, through remote contacts via phone apps, until physical meets was needed.

This group represent the very type of groups that the law makers of EU (EU (1), 2016) considered as the most vulnerable, when re-writing the 1994 Data Privacy Directive to the new GDPR regulation. Giving individuals like these a right to not be involuntary exposed, something that currently is very likely when using mobile services (Mansfield-Devine (1), 2012; Mansfield-Devine (2), 2012;Bradley, 2013; Kirk, 2013 ; Koskelainen, 2016).

Many commercial and free phone apps do scan the unit they get installed on, to collect non-affiliated data about the individual using the phone, to create marketing profiles or even more questionable mappings (Mansfield-Devine (1&2), 2012; Snyder 2014). A well discussed issue several years back, it now becomes more of a consideration, due to GDPR. We also seen knowledgeable criminals using the same technology to gain profit advantages. Particular Android 3:d party app stores, but even services like the free Spotify recently had attacks of rough apps tapping data or even encrypting devices for ransom (Markander, 2016).

Still, as shown by Le Dantec and others, we need this development to continue; for it clearly has, individually as from a society perspective, very beneficiary effects.

Yes, some of these groups will be seen as disruptive and a threat to the establishment, governments wanting to control and censor their communications (Glanz et.al, 2014), even in EU. However, we do not forbid motorbikes, though these is among the most dangerous traffic tools in the world, representing 23% of all road kills or being 29 times more dangerous than travelling with a car (Killi, 2014; Wikipedia, 2016).

Being human is a risk, independent what we are or do. Using tools will always be a risk that we, as Hardy has postulated, has to evaluate against its usefulness. Also when using ICT support. This author has been working with information security both as a side line and as main occupation for 32 years, we will never have a totally safe IT. Since designed and built by humans or with tools built by humans, IT always will have flaws; some easy to find, others less so. So we need to do the best we can, implement as good designs we can, introduce mitigations if possible and take the chance. So also here.

Those developing these services and apps, has a. to understand the risk they can introduce and b. to know the legal framework they have to consider [recognise here, GDPR do reach far outside the EU, legal actions can be brought in most of the world].

Based on this, there is a need to educate oneself to the rules controlling the development process and perform recommended mitigation actions available for the ICT tools used, to measure up to the GDPR legal framework. Doing so will considerably reduce the risk for both the users as the organisation delivering the service.

For the bad thing with GDPR, it fine structure is high, as high as €20M, even if only being an interest group or individuals serving one.

"But this is impossible to solve!"

No, it is about using common sense together with today well recognised processes and technology to, just, mitigate the risks. If having a core level of security, we can reduce the risk of breaches and fines to a so low level that it is acceptable within the EU regulation. Make no mistake, GDPR is a driver, changing European ITC usage for ever, it will be as profound as Sarbanes-Oxley Act (SOX) was for US ITC in the mid-2000:s. Anyone not noticing this will have a problem after May 25, 2018. And that is what this paper will discuss.

2. Research Process

This paper is a part of an advanced study course within Dept. Of Informatics, Linnaeus University, but also part of a larger project by the author. The course, 5IK502, has been discussing ethnography as a tool of developing new ITC support; how to use the knowledge of [hu]man and society to improve that ITC support. This author comes from the field of security praxis, which though often being regarded as a technical field, is very much about humans and culture, a sub-group of culture. Criminals is thinking humans.

Therefore, when starting this course, the idea was how to merge the two subjects into a paper, satisfying both the course, as the larger project. The key came through a request from a security fellow, asking the author to look into some consequences of the new European Data Privacy framework. The General Data Protection Regulation (GDPR) is replacing the 1994 Data Privacy Directive, where the EU Commission and Parliament have been deeply dissatisfied with the current implementation in the member states.

The author has chosen the subject area of activist and public service supported mobile services, one of the course's eight areas. This based on the current general focus at social media oriented ITC. A very interesting research area, both generally as from a security/GDPR perspective, with profound data privacy aspects.

We already know (Mansfield-Devine, 2012; Bradley, 2013; Kirk, 2013; Snyder, 2014; Luckerson, 2014; Markander, 2016; Koskelainen, 2016) that phone app manufacturer and government organizations has overstepped their boundaries, collecting vast amounts of data, without explanation or clear mandates. We now also see insurance companies issues health bracelets like Fitbits to customers, opening for a more continuously monitoring of their habits and maybe soon analysing blood and other medical components; tools reported as hackable (Shemkus, 2015).

Let's assert that this is a major topic area, needing a lot of more research than possible to do within the current context, concentrated to a singular case (Le Dantec et.al, 2011), extrapolating the effects of GDPR onto it and what can be done to mitigate the effects.

The author will not be denied that this approach pose a real limitation, where own study cases should have been included. But as earlier stated, after at talk with the CEO of Sweden's largest activist support group (UngMedia.se, personal communications), Sweden is currently not a suitable locality for field studies. Out of several reasons, Swedish Data Privacy laws (SFS,1998), among the more stringent in the EU, has cooled this side of the mobile service area down, as well as Sweden lacking a proper national digital identity, verifying users correctly in public contexts and thus generating a general weak public e-service market.

However, having a long personal practical experience, the author have experience of other cases related to the current topic area. Mainly, requested by employer's HR in 2007 to review the possible migration of all HR systems to a new global installation in Toronto, Canada.

Due to the German "Bundesverfassungsschutz die Personenbezogene Daten", this proved to be an impossible task, us to keep European data in Europe. The primary issue was the lack of non-repudiable approvals from all employees, allowing export to outside EU. The experience from these proceedings has been extrapolated to give a possibility to evaluate realistic consequences, when applying GDPR on activist and public mobile e-services.

Other text sources has been included, to give an in-depth understanding of the issues at hand, particular in the perspective of World Economic Forum/McKinsley (WEF, 2014) and FBI (FBI, 2015) calculating a steep rise of data oriented criminality toward the mid 2020:ies, WEF estimating we will requiring some $3 trillion to protect our data; affecting world economy. With the risk that our data (EU (1), 2016) no longer will be ours.

3. Case - Homeless Shelter ITC support, a 2016 possible approach.

Le Dantec et.al. (Le Dantec, 2008, Le Datec et.al., 2011, Asad & Le Dantec, 2015) have for half of decade followed the use of ITC and mobile solutions in the context of supporting socially marginalised individuals, with a study of a shelter for homeless mothers as the prime example (Le Dantec et.al., 2011).

When implemented as a Georgia Tech project in the late 2000:s, the principal solution was a simple bulletin board at the shelter, supported with cheap SMS messages. A solution then security-wise robust and with minimal risks, since GSM and CDMA2000 phone protocols is inherently encrypted transport protocols. Though having issues today, to breach these protocols at the time, one had to breach the phone companies or establish an economical substantial effort to analyse large data sets for a single phone's encryption keys (Farnham & Fuller, 2010), not likely at the time and case of the Georgia Tech experiment.

Today the situation is far different and substantially more risky, most having a smart-phone, using a multitude of apps. If implemented today, Georgia Tech likely had rented Amazon Cloud Server, built a web based solution and an app, distributed to the mothers at the shelter. A perfect customer adapted solution, like many other purpose-built apps at Apple and Google stores. Solving the task with efficiency and needed privacy of the "customer", but with issues.

To this, we need to transplant the whole case to Europe, under the GDPR framework (EU (1), 2016), to analyse the effect of the new protective framework on the discussed type of ITC usage (current case and/or activist networks). The key with the GDPR framework is really two-fold, "Security by Design" and "Who accessed what data and when/where".

- “Security by Design”

  Anyone designing a solution, even if on paper only, to operate within the bounds of GDPR, need to respect some basic demands. How to control who can access the information and keep a track record of when, where and how. Non-repudiable.

  It does not matter how we store or process the information, we need at every instance to understand where EU protected data are, who can reach it there and when and how. We need a data-flow map of the data, showing all this.

  This means that the team has to begin to draw the data-flow map and identify access needs and risks along the way (Badr et.al, 2011; Soomro et.al, 2016; Magnusson, 2016). Based on the data-flow map and the identified access points and risks, a basic system design can be developed.

  Not doing this can be a fineable audit point, the day EU defines how the following of GDPR shall be reviewed. From now, all process and system documentation need to be described out of this principal clause.

- Practical security

  If we set any paper process aside, looking at ITC followings needed to satisfy GDPR, we have four main areas to review. a. design and programming of the code, b. secure the data flow, c. secure the data storage, and d. access control.

  GDPR put clear demands on how to perform these and in some instances the solution is to have proper encryption on both communication and data storage. Fact is, even if losing

a lot of personal data, if the victim can show that data been subject to modern encryption practice, data not possible to be read by the offending party, no legal action will be expected (EU (1), 2016).

Having a proper mitigation strategy in place is the first step towards making the organisation GDPR conformant. With such a strategy in place, though not having finished remediations by May 25, 2018, an operational strategy and project plan is step one in the defence against becoming liable (Ed., 2008; Hayden, 2010; Badr et.al, 2011; Sen&Borle, 2015; Soomro et.al, 2016). But let's review each of the four bullets in their context of our case.

- Design and Programming

For the last 16 years Sans Institute and the OWASP interest group have each published a list of vulnerabilities in programing and web development. SANS Top 25 and OWASP Top 10 (Christey, 2011; Owasp, 2015). In principle, it is the same objects since 2001, even if they do trade places in the lists.

Unfortunately these lists do point to a very severe and systematic deficiency within the ITC community, we do not learn by our mistakes. Spending 14 years in automotive industry, with very structured quality programs, the ITC sector still is at a 1940 quality consciousness. The questions of software quality have been addressed several times, such as by Kernighan and Plauger (1974 & -76), Kernighan and Pike (1999) as well as by Fred Brooks in his monumental "The Mythical Man-Month" (1982). Sadly, none of these giants is part of the programming curriculum around the world.

ITIL and other frameworks, as COBIT, was to address these issues, but as SANS and OWASP yearly proves, as well as major incidents shows, we see no improvement in real world (WEP, 2014; FBI, 2015; Hardekopf, 2015; Riley&Pagliery, 2015).

GDPR here forces us to look at the listed vulnerabilities, how to mitigate them. For there exist plenty of examples how to remove these risks from the implementations. So our case team have to sit down, before starting coding, reviewing possible actions to implement into their solutions.

- Secure the data flow

One of the key components of GDPR is to know where data are at a given time and how it got there as well as where it is going and why. This a concept familiar for anyone working SOX remediations (Wiki (1), 2016; Wiki (2), 2016).

In order to establish if data has been manipulated, we first need to know where it's been and where it is sent as well as who accessed it and why. Standard audit procedures. As mentioned earlier, this need to go in to our cases design phase (Magnusson, 2013), identifying where data passes and how to security both in transit as in the applications and storage (Kindervag, 2012; Magnusson, 2016).

With the background of so many smart-phone apps today doing "drive-by" data collecting [asking for rights to phone book and SMS etc] (Mansfield-Devine (2), 2012; Bradley, 2013; Kirk, 2013 ; Koskelainen, 2016; Markander, 2016); in retrospective of the

intended case, question is if a smart-phone really can be used for any data sensitive solutions.

The short answer is; yes they can. But the application developer must implement some procedures to hinder other apps to collect its data. This include using https for communication with the central application or using other proven encryption protocols and application firewalls (Magnusson, 2009; Magnusson, 2013; Magnusson, 2016); not home-brewed solutions, that always been proven to be hackable.

- Secure the application

But to this, running an app means that we need to encrypt the app on the phone, the program stack and run memory. By using a proven encryption tool pack for the application language used (Mansfield-Devine (1), 2012).

This, so if the "client's" children download a game app from an uncontrolled source [not to uncommon] the shelter application still is protected from both data skimming as communication breaches. Including phone Trojans not being able to infect the shelter central application with malware, since it cannot follow the communication and inject its content (Abraham&Chengalur-Smith, 2010).

But once again, this put stress on the developers, they have to have better knowledge and tools than what is baseline today (Spafford, 1997; Spafford, 2001; Spafford 2009).

- Secure the data storage

However, the most important effect of GDPR, is that we need to encrypt data storages. Both in the apps as on disk. It is the one most effective protection solution. An encrypted data storage, protected when extracted, is an EU "walk free of jail" card. The GDPR says directly, encrypted data lost, if no way to open it, it is not even needed to report the loss (EU (1), 2016).

What encryption is dependent on what operating system and storage solution used. In the case of the shelter system, if using an Amazon virtual environment, it is a case of using Linux or Windows. Though several choices, there is Linux EncFS (Encrypted File System), also found in a windows version, Windows Bitlocker and, though there is some growing concern that US government succeeded to retrieve an escrow key, Truecrypt. Some SAN and NAS applications have their own container encryption, to that.

A hard choice, but well worth the effort, since data loss via lost disks or data containers will be legally nullified. Also, since we're talking Amazon, which together with MS Azure and Google have an issue, that a customer instance can be relocated anywhere in the world, which we need to review and evaluate (Lindström et.al., 2015).

However, an encrypted processing instance, also having encrypted communication and storage, can be run anywhere in the world; as long as the controlling encryption key only reside within EU. If the process container and its communication is using modern encryption methods, it will be sufficient protected, even if processing EU personal data outside the EU.

- Access Control

  The single most common cause for data loss, access to the system. Faulty access control stands for the majority of all data crimes, internal as external. Not having a good authorisation nor access control solution, will counteract any other actions to secure data. Something identified in most audits (Magnusson, 2014).

  GDPR do require the same level of authentication and authorisation as the Sarbanes-Oxley Act of 2002, SOX (Wiki (1), 2016) or in the banking regulation for PCI-DSS (PCI, 2016). Knowing who accessed what and when as well as why, will from May 25, 2018 be a crucial information, which has to be proven via non-repudiated logging of the accesses.

  The person with valid access, even if a stolen access, will always be able to reach the data we want to protect. So, today simple passwords is not enough. And if using an open smart-phone situation is even more critical. Most people hate their phone's access control, pin code or whatever, many disabling them. GDPR demands us to take this to a new level, 2-factor authentication, like Google's 2-Step verification (Google, 2016), but undoubtedly the shelter users will not go this way.

  Best is if they use a phone with a pattern verification. A pattern with 12 dots or more to connect right to get access. If not able at least a PIN code. The users has to accept that no authentication is a no-show in using the service.

  At server/administration side, Google 2-factor or password key fobs like Yubikey is a minimum.

- Logging

  We often see logging as a costly inconvenience. However, finding out who did what and when, requires a full logging of all access points, from the smart-phones to server logins. And these has to go to a log server, none of the administrators has access to. As the key part of access control, it has to be un-tamperable. When the GDPR auditors come, we need to give them a clean record.

  The issue is how. In our shelter case, I would look for an ITC security firm, willing to do the logging. A 3:d party storing and analysing the access data. More costly, but in the retrospect of fines up to €20 Million, well it is a cost worth taking.

When looking at the requirements, they seem daunting, how to solve this. Let's step through the case, to look at the effect of the law on the solution. As seen, there is a lot of actions we can do to reduce the risk, albeit not favourable to any CFO.

But as said above, most of these costs need to be balanced toward the total risk. We will not see a public service like our shelter example to top up a €20M fine, not likely even a €3-400.000 fine, but a fine of €100.000 is definably within the possible boundaries, possible to kill a worthy project.

Said before, we have a lot of the solutions needed by looking at older SOX and/or PCI-DSS "playbooks". EU based ITC have for those scenarios been solving the same issues for nearly 1.5 decade by now, so no surprises, just hard work doing it right. The actions above is just a scratch on the surface to show what can be done, using well-known remedies.

4. Analysis

Do the shelter case need to shut down May 25, 2018, if in Europe?

No, if it spend some of the risk money on its security infrastructure, observing lessons learnt from SOX and PCI-DSS, it can continue as it done so far.

We do have enough knowledge to being able to mitigate GDPR, have had for over a decade. This isn't the "The Emperor's New Clothes" (Andersen, 1837), it is more "The Same Procedure as Every Year" (NDR, 1963). There is nothing new with GDPR, it is much the same regulation as EU took in 1994, in the EU Data Protection Directive.

There is some strengthening due to the technical and market changes, but by and large it is a workable regulation, based on Best Practice. And it is a good regulation, handing over the ownership of all Personal Data to the individual being described. Without any geographic limitations, where the data is "mined" (EU (1), 2016; EU (2), 2016).

EU is keeping its right and liberty to prosecute any misbehaviour by data collectors, even outside the EU. Thus GDPR is a game-changer, giving the individual rights of his/her own data and the "Right to be forgotten" (EU (1), 2016).

As mentioned, the idea of this type of social support (Le Dantec, 2008; Le Dantec, 2011; Le Dantec, 2015) is the future in the way of society to help marginalised groups; even if it today is more of a US or 3:d world phenomena (Banks, 2013; Balch, 2014, UN, 2015, Pendse, 2015) of support.

ITC do need to learn from manufacturing, regarding quality and security. It need to learn from mistakes done and being repeatable in its design in a positive way, away from the SANS and OWASP pitfalls (Christey, 2011, OWASP, 2015), but also issues addressed generally as in Brooks "Mythical Man-Month" (Brooks, 1982). His super team with a secretary keeping track of the work, the main programmer with his/her sparring partner, the support programmer and the "librarian", keeping track on the group's common routines.

Having seen such a team in reality during two years, spending hours discussing it with the team leader (PKA, personal communication, 1987-89), supporting him with infrastructure, he used Brooks solution template in building a finance system, proving Brooks theorem as the essence of the software industry. What we still misses after 60 years of IT.

Another reflection was done in the early 1990:ies, "The knowledge gained from failures is often instrumental in achieving subsequent successes", sited by D.A. Gavin (Gavin, 1993) in his book about building learning organisations. The funny thing is, having spent 14 years in automotive and a total of 8 years as consultant and another 10 years as CIO, TIO and CS teacher, this author still wonders where the learning organisations within ITC are. Critical in manufacturing, but totally lacking in ITC.

With Kaizen, Six Sigma and all other methods used in manufacturing we should have a solid lead; but though people like Ed Yourdon, the "Three Amigos", Booch, Jacobson and Rumbaugh, Brooks and others, we're still lacking. We have no clue how to standardise ITC development.

5. Discussion

As noted in the last section, we're still at fault (Tashi & Ghernaouti-Hélie, 2007; Kindervag, 2012), coming to how we develop our ITC solutions. Grand plans give away to agile development. Brooks, Yourdon and a lot of others defined the process as 70% analysis and 30 % development. Agile methods is 100% development.

It do have its merits, it gets slow projects going, something I see every day in my work. But where is the after-though, where is the guiding principle, what problem is being solved? Remember Hardy?

Probably over 90 % of our security issues comes from solving a practical issue, without reflecting over its consequences. Yes, that nice customer person telling us how he/she like to work gets his/her problem solved. But at the cost of creating an open barn door, for any hacker or internal perpetrator to use (Ed. 2008,).

Ed Yourdon had his idea about "Structured Walkthroughs" (Yourdon, 1978), to have a team review the solutions structurally, already in the late 1970:ies. In +30 years this author never seen such a walkthrough performed, though I tried to implement them myself a couple of times. But during my time in automotive, I have a couple of times experienced the process within car projects, where they are mandatory reoccurring error correction methods. About once a week in most sub-projects.

GDPR is not a lemon, it is nothing we can hid from and it is no disaster; as long as we use proven methods to mitigate and remediate the deficiency's we do have in our ongoing ITC environments. We just have to stop thinking within the box.

If we do, we fail to see the big picture. A topic the British military psychologist, N.F. Dixon, touched with a frightening clarity in his book, "On the Psychology of Military Incompetence" (Dixon, 1976). Though Dixon only used pre-1950 military cases, his wisdom is universal. As man[kind] we are no better than our preconceptions and thus strongly failing regarding analysing the issues at hand. Again automotive is the proven ground, today most recalls are software, not the basic mechanics.

At the same time, GDPR is a once in a lifetime chance to rebuild our ITC to something that better support our operations, getting rid of old stuff, to understand our data flow and correct the flaws built in during the last 3-4 decades (Magnusson, 2016). To reuse that SOX/PCI-DSS knowledge in an innovative and secure way, starting with security, instead of mounting it on top as a back-pack.

6. Conclusion

In an increasingly politically and social polarised world, the value of using new tools to support marginalised groups is important. Stagnant societies never evolves, it the thinking outside the box that has brought humankind to where it is today. For better and for worse.

We live in a time that George Orwell probably would felt much acquainted to. We're needing our Winstons (Orwell, 1949), people that challenge or turn the tide of our society, like the middle-east activists did 2010-13. Thinking out of the box, producing new ideas, showing a new middle-east with their Facebook and Twitter driven "revolutions" in Tunisia, Egypt and Libya. They failed, yes, for now.

The case used for this paper is an example of what we will see in the coming years; teams positively engaging previously weak marginal groups in society, taking lead from Facebook, Twitter, Uber and other commercial actors, re-inventing solutions for more sturdier support than these target groups had in the past.

Smart-phones being a crucial part of this, more important than tablets or laptops. The "customer" own his/her own supportive tool, able to store important information in a longer perspective, as well as readily available and with better access to supporting services. As Le Dantec (Le Dantec et.al, 2011) formulates it, "The technology is not the solution but rather the means for users to articulate their attachment to an ever evolving set of issues". The smart-phone becomes an extra "hand".

But this also places the technology in a sensitive position. Suddenly we go around with tools, able to tell others a lot about us, making the tool a risk. EU has recognised this, when formulating the General Data Protection Regulation, making the "Security by Design" the critical part of the regulation.

We do not need to know the full regulation, it is enough to recognise this; "Keep data secure", "Know where data flows, why and on decision by whom" and "Who accessed what data, where and when" and maybe the most important, "A EU resident owns all data describing him or her, independent of who collecting it and where", including "The right to be forgotten". Five key statements that from May 25, 2018 will drive all ITC treating any form for EU citizen data. Failure to observe these will result in EU fines, independent of our objective and financing. We need to safeguard the data we are entrusted with (Badr et.al, 2011; Kindervag, 2012; Soomro et.al, 2016).

We no longer can say, "This is not my problem", for EU made it our problem. Independent if a global conglomerate, a "mom & pop" operation, a public service or an activist group, we need to review our intentions, processes and technical designs. We need to facilitate EU's "Security by Design" at the core of our operations. But will we be able?

Having worked ITC for +30 years, no, we're nowhere near. A key issue is the lack of security competence. Professor Gene Spafford at Purdue Univ. has addressed the problem towards the US Congress more than once (Spafford, 1997; Spafford, 2001; Spafford, 2009). Apart from an initiative between some UK universities and ISC2.org, information security is still an additional, not a core topic, in most university curriculum's. As in most organisations, just an uninteresting backpack, weighting everything down. But EU says, "no more".

Information security and securing the data flow has to be a substantial part of the first year curriculum, if academia is to retain its trustworthiness out in the "real world". Not having courses in information security or GDPR will be a sure route to failure for students, just as lack of Java or Javascript is today. If the students have the ability to build secure processes and mitigate flaws like the SANS and OWASP vulnerabilities, they will be an integral part of protecting their employers and, in some cases, their clients ability to satisfy EU-GDPR.

7. References

Books:

Andersen, H.C., 1837, "The Emperor's New Clothes", Sept 1837, C.A. Reitzel, Copenhagen, Denmark

Brooks, F.P., 1982, "The Mythical Man Month", Addison-Wesley, Reprint edition

Dixon, N.F., 1976, "On the Psychology of Military Incompetence". Jonathan Cape, London

Ed., 2008, "Data Breaches Trends, costs and best practises", IT Governance Publishing, Ely, UK

Hardy, G.H., 1967, "A Mathematician's Apology", Cambridge Univ Press, London, UK

Hayden, L., 2010, "IT Security Metrics : A Practical Framework for Measuring Security and Protecting Data", McGraw-Hill, NY, US

Kernighan, B.W., Plauger, P.J., 1974, "The Elements of Programming Style", McGraw-Hill, New York, 1974

Kernighan, B.W., Plauger, P.J., 1976, "Software Tools", Addison-Wesley Professional; 1 edition (January 11, 1976)

Kernighan, B.W., Pike, R., "Software Tools", 1999, Addison-Wesley; 1 edition (February 14, 1999)

Orwell. G., 1949, "1984", Secker & Warburg, London, UK, 1949.

Pendse, P.H., 2015, "Business Analysis: Solving Business Problems by Visualizing Effective Processes and IT Solutions", Nov 30, 2015, PHI Learning, New Dehli, India

Yourdon, E., 1978, "Structured Walkthrough", 1978, Yourdon Press

Reports:

Asad, M., Le Dantec, C.A., 2015, "Illegitimate Civic Participation: Supporting Community Activists on the Ground", CSCW, March 14-18, 2015, Vancouver, BC, Canada, ACM

Federal Bureau of Investigation, "Internet Crime Complaint Center (FBI)", 2015, 2014 Internet Crime Report, FBI, Washington, US

Kindervag, J., 2012, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research, Cambridge, MA, US.

Le Dantec, C.A., Farrell, R.G., Christensen, J.E., Baily, M., Ellis, J.B., Kellog, W.A., Edwards, W.K., 2011, "Publics in Practics: Ubiquitous Computing at a Shelter for Homeless Mothers", ACM/CHI, May 7-12 2011, Vancouver, BC, Canada

Le Dantec, C.A., 2008, "Life at the Margins: Assessing the Role of Technology for the Urban Homeless", ACM, v15, Iss5, p24-27, ACM, New York, NY, US

Lindström, J., Magnusson, L., Sporrong, P., Berglund, U., et. al., 2015, "En praktisk och lite enklare checklista för införskaffande, användning och lämnande av molntjänster", CSA Sweden, CSA, SE

Magnusson, L., 2009, "A Security Practitioner's view on Internet Protocol"s, Sept 26, 2009, IETF, IETF Draft Series, "draft-magnusson-secure-practice-00", IETF.org

Spafford, E.H., 1997, "One View of A Critical National Need: Support for Information Security Education and Research", COAST Project and Laboratory", 105th Congress, US Senate Committee on Commerce, Science and Transportation, revised July 17, 2000.

Spafford, E.H., 2001, "Cyber Security -- How Can We Protect American Computer Networks From Attack", 107th Congress, US Senate Committee on Commerce, Science and Transportation, Oct 10, 2001.

Spafford, E.H., 2009, "Cyber Security: Assessing Our Vulnerability and Developing an Effective Defence", 111th Congress, US Senate Committee on Commerce, Science and Transportation, Mar 19, 2009.

Tashi, I., Ghernaouti-Hélie, S., 2007, "Security metrics to improve information security management", Proceedings of the 6th Annual Security Conference, April 11-12, 2007, Las Vegas, NV, US

World Economic Forum/McKinsey & Company (WEF), Jan 2014, "Risk and Responsibility in a Hyperconnected World", Geneva, CH

Articles:

Abraham, S., Chengalur-Smith I., 2010, "An overview of social engineering malware: Trends, tactics, and implications", Technology in Society, Volume 32, Issue 3, August 2010, p183–196, London, UK.

Badr, Y., Biennier, F., Tata, S, July 2011, "The Integration of Corporate Security Strategies in Collaborative Business Processes", IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 4, NO. 3, p243-254

Magnusson, L. as "Magnusson, K.", 2013, "Informationssäkerhet på 2010-talet", Chapter 12.3, Bonniers Ledarskapshandböcker, Stockholm, SE

Magnusson, L. as "Magnusson, K.", 2014, "Auktorisering-accesskontroll som nyckel till bättre IT-säkerhet", Chapter 12.6, IT-management, Bonniers Ledarskapshandböcker, Stockholm, SE

Magnusson, L, 2016, "Integration as Secure IT Architecture Driver", May 2016, Course report 4DV505 - Current Topics within Computer Science, Dept. Of CS, Linnaeus University

Sen, R., Borle, S., 2015, "Estimating the Contextual Risk of Data Breach: An Empirical Approach", Journal of Management Information Systems. Fall2015, Vol. 32 Issue 2, p314-341.

Soomro, Z.A., Shah, M.H., Ahmed, J, 2016, "Information security management needs more holistic approach: A literature review", International Journal of Information Management, Volume 36, Issue 2, April 2016,

p215–225

Web Articles:
Balch, O., 2014, " Four mobile-based tools that can bring education to millions", Aug 20, 2014, The Guardian, London, UK as viewed Dec 2, 2016; https://www.theguardian.com/sustainable-business/2014/aug/20/mobile-phones-smartphone-education-teaching
Banks, K., 2012, "Mobile Learning: How Smartphones Help Illiterate Farmers in Rural India", June 5, 2012, National Geographic as viewed Dec 28, 2016; http://voices.nationalgeographic.com/2012/06/05/mobile-learning-how-smartphones-help-illiterate-farmers-in-rural-india/
Bradley, T., 2013, "Dropbox is peeking at your files", CSO Online, Sep 13, 2013, as viewed Apr 5, 2016; http://www.csoonline.com/article/2137123/privacy/dropbox-is-peeking-at-your-files.html
Chacos, B., May 5, 2014, "Antivirus is dead, says maker of Norton Antivirus", PCWorld, as viewed Jan 11, 2016; http://www.pcworld.com/article/2150743/antivirus-is-dead-says-maker-of-norton-antivirus.html
Christey, R. (Ed.), 2011, "2011 CWE/SANS Top 25 Most Dangerous Software Errors" ,CWE/Sans.org, as viewed Mar 30, 2016; http://cwe.mitre.org/top25/
Farnham, G., Fuller, K., 2010, "GSM Risks and Countermeasures", Feb 1, 2010, Sans Institute, as viewed Dec 25, 2016; https://www.sans.edu/student-files/projects/201004_30.pdf#__utma=216335632.856143714.1482664533.1482664533.1482664533.1&__utmb=216335632.5.8.1482664562270&__utmc=216335632&__utmx=-&__utmz=216335632.1482664533.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)&__utmv=-&__utmk=175301985
Garvin, D.A., 1993, "Building a learning organization.", Harvard Business Review. Jul/Aug1993, Vol. 71 Issue 4, p78-91. as viewed Dec 2, 2016; http://eds.b.ebscohost.com.proxy.lnu.se/eds/pdfviewer/pdfviewer?sid=6d68b741-e7d3-40c9-b596-f1bf028e2986%40sessionmgr120&vid=3&hid=108
Hardekopf, B., 2015, "The Big Data Breaches of 2014", Forbes, Jan 13, 2015, as viewed Mar 16, 2016; http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#f6250f33a48f
Kille, L.W., 2014, "Transportation safety over time: Cars, planes, trains, walking, cycling", Oct 5, 2014, Journalistsresource.org, as viewed Dec 25, 2015; https://journalistsresource.org/studies/environment/transportation/comparing-fatality-risks-united-states-transportation-across-modes-time
Kirk, J., 2013, "Dropbox takes a peek at files. But it's totally nothing, says Dropbox", IDG News Service, Sep 13, 2013, as viewed Apr 6, 2016; http://www.pcworld.com/article/2048680/dropbox-takes-a-peek-at-files.html
Koskelainen, A., 2016, "Säkerhethetshål hittat I populär Android-app - miljontals telefoner I riskzonen", Dec 2, 2016, IDG Techworld, as viewed Dec 2, 2016: http://techworld.idig.se/2.2524/1.671017/android-app-airdroid
Luckerson, V., 2014, "7 Controversial Ways Facebook Has Used Your Data", Time Magazine, Feb. 4, 2014, New York, NY, US, as viewed Apr 5, 2016; http://time.com/4695/7-controversial-ways-facebook-has-used-your-data/
Mansfield-Devine (1), S., 2012, "Android Architecture: attack the weak points", October 2012, Network Security, US, as viewed Dec 2, 2016; http://www.sciencedirect.com.proxy.lnu.se/science/article/pii/S1353485812700922
Mansfield-Devine (2), S., 2012, "Android Malware and Mitigation", November 2012, Network Security, US, as viewed Dec 2, 2016; http://www.sciencedirect.com.proxy.lnu.se/science/article/pii/S1353485812701046
Markander, M., 2016, "Spotify beskylls för skadlig kod", Oct 5, 2016, IDG M3, Sw, as viewed Dec 2, 2016; http://m3.idg.se/2.1022/1.666936/spotify-beskylls-for-att-sprida-skadlig-kod
Murphy, E.A., 1949, "Murphy's Law", Murphy's Law Site, US http://www.murphys-laws.com/murphy/murphy-true.html
OWASP, 2015, "OWASP Top 10 Vulnerabilities", OWASP.org as viewed Mar 30, 2016; http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf
Riley, C., Pagliery, J., March 19, 2015, "Target will pay hack victims $10 million", CNN Money, as viewed Feb 4, 2016; http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/
Shemkus, S., 2015, "Fitness trackers are popular among insurers and employers – but is your data safe?", April 17, 2015, The Guardian, UK, as viewed Dec 25, 2016; https://www.theguardian.com/lifeandstyle/2015/apr/17/fitness-trackers-wearables-insurance-employees-jobs-health-data
Snyder, B., 2014, "User Beware: That Mobile App is Spying on You", IDG CIO, Aug 5, 2014, as viewed Dec 25, 2016; http://www.cio.com/article/2460616/mobile-apps/user-beware-that-mobile-app-is-spying-on-you.html
Whittaker, Z, May 5, 2014, "Symantec calls antivirus "doomed", as security giants fights for survival", ZD Net, as viewed Jan 11, 2016; http://www.zdnet.com/article/symantec-calls-antivirus-doomed-as-security-giants-fight-for-survival/

Other sources:
SFS (Svensk Författningssamling), 1998, "Personuppgiftslagen", Apr 24, 1998; https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204
EU Council (1), 2016, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL", April 27, 2016, Official Journal of the European Union, 4.5.2016,L119/1
EU Council (2), 2016, "Press Release:Questions and Answers Data Protection Reform, As viewed Nov 10, 2016: http://europa.eu/rapid/pressrelease_MEMO156385_en.htm
Google, 2016, "2-Step verification", support.Google.com, as viewed Dec 28, 2016; https://support.google.com/accounts/topic/7189195?hl=en&ref_topic=3382253
Norddeutscher Rundfunk, 1963, "Dinner for one", NDR, as viewed Dec 28, 2016; https://www.ndr.de/unterhaltung/comedy/dinner_for_one/
PCI, 2016, "PCI Security Standards", as viewed Dec 28, 2016; https://www.pcisecuritystandards.org/
PKA, 1987-89, Personal Communications with Finance Team Lead, Johnny Johansen, PKA.dk, Copenhagen, Dk
UN, 2015, "One Million Smartphone-Enabled Community Health Workers in Sub-Saharan Africa", UN SDSN, UN, New York, NY as viewed Dec 28, 2016; http://unsdsn.org/what-we-do/solution-initiatives/chw/
Wikipedia, 2016, ""List of countries by traffic-related deaths rates", Wikipedia, as viewed Dec 25, 2016; https://en.wikipedia.org/wiki/List_of_countries_by_traffic-related_death_rate
Wiki(pedia) (1), 2016, "Sarbanes-Oxley Act", Wikipedia, as viewed Dec 27, 2016; https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act
Wiki(pedia) (2), 2016, "Information Technology Controls", Wikipedia, as viewed Dec 27, 2016; https://en.wikipedia.org/wiki/Information_technology_controls

Meeting Procedings:
(ISC)2 SecureScandinavia 2015, Stockholm, SE
Hart, J., May 19, 2015, Speach, "Virtual World Exposed: Hacking the Cloud", Gemalto-Safenet, US
Hansen, J., May 19, 2015, Speach, "Defending Against Phishing Attacks: Case Studies and Human Defenses", PhishMe