National investment for boosting cyber readiness

The European Union is taking a series of measures to increase the resilience and preparedness of cyber security. Already in 2013, the European community defined a series of objectives and actions aimed at reducing cybercrime by developing a self-defense capacity and directing the industries of the towards a coherent policy of development of the sector. In 2001 the NIS directive is the first fundamental step to promote a culture of risk management, the directive introduces in fact the mandatory safety requirements for the main economic operators, in particular for all operators providing essential services.

In the meantime, the series of cyberattacks is lengthening and whenever the impacts are significant, new requests for the intervention of the legislator are invoked through laws and regulations. It is now clear to everyone that today's society is becoming increasingly dependent on digital and cyber-attacks can create large-scale damage. The legislative intervention should move from the assessment and understanding of the monetary costs that society is willing to support as well as understanding the level of the threat.

Costs that can then be supported by consumers, through higher prices, by the legislator or by companies. To this we should add the awareness that national investments, such as defense are difficult to evaluate in a purely objective way. Furthermore, it should be noted that IT security investments are recurrent. Products and software are like buildings, they have an initial design cost and a maintenance cost. A further reflection must then be made on the theme of usability. Normally, the security systems affect the user usability, we see, for example, how many interactions in some applications, are requested to authenticate a user. In the digital scenario usability and simplicity will be for succeeding, business cannot accept limitation of the user's flexibility.

A noteworthy topic is dissuasion, which is particularly complex in the domain of cyberspace with respect to the analogous physical world. Deterrence depends on being able to attribute acts to persons or institutions and therefore to punish the guilty. The attribution of cyber attacks on a network is difficult, sources can be falsified or rewritten along the way. The attribution therefore requires an analysis that is often very expensive. Punishing attackers then can be problematic as they can work outside the jurisdiction of the government where their target is. Are we ripe for a discussion involving private public investments to support IT security? Can we quantify, taking into account the various aspects, the value to be invested at national level? I believe that today the time is ripe to start a national dialogue that inserts this theme in the logic of investment in the country involving in this process the companies and operators in the sector...

Enjoy your reading!
Nicola Sotira
General Manager GCSEC
Data portability: the advantages and disadvantages of information’s immateriality
by Marco Fiore – GCSEC

Impact of GDPR on Biometric Systems
by Paul Guckian – Lead Software Developer at Delaney Biometrics

GDPR, a real opportunity for a new digital revolution
by Marjola Begaj – Affiliate Member of International Compliance Association UK

Data portability: the advantages and disadvantages of information’s immateriality
by Marco Fiore – GCSEC

It is known that the role GDPR within European regulatory systems, is a major player like the fundamental rights of every member state. The recognition of the Regulation, in fact, extends the application contexts of the law concerning the safety and security of the data, and it obviously increases its protection.

One of the most interesting and central aspects of the GDPR innovations introduced is certainly the right to data portability at art. 20 of the Regulation (EU) 2016/679. When we talk about “data portability” we want to describe the possibility of transferring and requesting data processed by a data controller, or another data controller when duly authorized, and those data are transferred to third parties or/and communicated to the person concerned. Simply is the right to receive the data previously provided to a holder to keep them in view of a further use, or even to obtain the transmission of data from one holder to another. The implementation of the regulation of data protection is intended to expand those data standards that until now, have been the foundation of the era of computerization developing security protection of personal data, particularly as indicated by art. 8 of the CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

In sociological perspective instead is aimed at encouraging the digitization of citizens but also data portability facilitates the fundamental EU principle of law of the “free movement of people, capital, goods”, but also data itself.

Which data are under the right to data portability:

The right to data portability exists only if the data are processed with the consent (art. 6, 1, letter (a) and art. 9, letter (a)) or on the basis of a contract (art. 6.1, letter (b)).

Portability is obviously excluded if the treatment is carried out for the performance of a public duty or in the exercise of public authority (art. 20.3).

These assumptions emphasize the predominant role of the bind that needs to be established between the owner and concerned. Like in the broader and granite foundation principle of the free determination of will contract, those provisions are designed to emphasize the expressed principle of the dominant position of data subject ‘right upon data controller authority. It will be interesting to understand deeply the contractual liability of the owner or person responsible for the treatment in front of the formalized expression consent in an agreement between the parties (art. 6.1, letter (b)). An important element to underline is that portability is referred only if the treatment is based on electronic processing unit (not paper) to facilitate data portability in the EU.
In all other cases it does not apply, such as for treatments based only on legitimate interests. The GDPR covers data "provided" by data subject. Therefore, it is limited to personal data only and it does not apply to anonymous data, but instead, it applies to pseudonymous data, since those are clearly linked to personal data.

Referring to anonymized data, we have to emphasise that art. 89 GDPR “Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes” deals with “Inferred Data”. The "new-created" data by the controller are not the subject of the right to their portability because they are not "provided directly by", although they may be or may be related to him. The article, in fact, establish some derogation at the data portability: “Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes”.

According to the interpretation of WP29 (European Data Protection Board), the term "provided" should be interpreted in a broad sense, so the intent of the legislator is not limited only to personal data communicated by the data subject (eg. Email address), but also extends to personal data generated (observed) by the activities of the data subject (eg location data, history of searches, browsing data, the heartbeat recorded by a device). On the other hand, the data generated by the data controller are not included on the basis of the analysis of data provided or collected by the data subject autonomously (inferred and derived data, eg credit score or data analysis), or obviously data obtained from third parties. Instead, agreeing to the European Commission’s viewpoint, the goal is to guarantee personal data in social networks, and therefore with not only those operations of data entry that is a reductive interpretation of the term "provided".

With reference to Article 20

1. “The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided ...”. Are not mentioned information about the specific machine-readable format but it is assumed that the data holder should do an assessment of interoperability of the format with other services (eg. a PDF can not be processed easily by the data subject.) but also specify the assessment measures of portability in its DPIA (Data Protection Impact Assessment)1.

2. “In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.”. The only reason, therefore, a data controller can refuse to comply with the provisions of art. 20, paragraph 2, is the excessive technical complexity, or even the impossibility of transferring the data to the other controller indicated by the data subject at fist.

Finally point 4. of art. 20 also establishes that the exercise of the right to data portability must not damage the rights and freedoms of others, which is also fundamental in the perspective of several appointed owners and of data that affect more than one person.

Data communication and portability deadlines

For data portability: “The controller shall provide information on action taken on a request under Articles 15 to 22 the data subject without undue delay and in any event within one month of receipt of the request. 2 That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. 3 The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. 4 Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise

---

1 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 – Annex 2 – Criteria for an acceptable DPIA p.22
The GDPR and the Act are henceforth (integrated) to UK companies which process data in ways that bring them within its scope, even if they are not established inside the EU, including subject rights such as the data portability. The GDPR and the Act are both enforced by the Information Commissioner (the same institutional role of Garante per la protezione dei dati personali in Italy) through the Information Commissioner’s Office, or ICO and the GDPR regulation will continue to be enforced by the ICO.

The GDPR includes provisions that enable the European Commission to issue a decision of adequacy where a country is able to demonstrate that it has adequate data protection laws, and an independent and effective data protection authority. It would be possible for controllers in EU to freely transfer personal data to the approved third country as though it were another Member State. The UK would appear to be, according to the GDPR regulations, theoretically an appropriate country. However this adequacy criterion can not fail to take into consideration the political evaluations of the case, which necessarily complicates the issue. Moreover the criteria sought by the UK would be different to any other third state. It would be a condition of adequacy “strengthened”, because of the role of the English ICO that is trying to get the formal assignment to continue participating in the European Committee for Data Protection, which aims UK to ensure the consistent application of the law.

The possible outcomes of the UK’s situation are three:

No deal: The UK becomes a third country, to which EU Member States may not transfer personal data unless there is a legal data transfer solution in place (explained below).

Adequacy decision: The UK is recognised as an approved country, to which personal data may freely be transferred from EU Member States. However, the ICO would not participate in the European Data Protection Board, which could result in an inconsistent approach between the ICO and European regulators.

Enhanced adequacy decision: The UK is recognised as an approved country and the ICO would participate in the European Data Protection Board. Needless to say, this proposal by the UK government has met resistance from the EU.

In a recent interview Euronews, caught up with British Minister for Digital and the Creative Industries Margot James that Europe’s Web Summit, UK has “absolutely no intention” of changing the General Data Protection Regulation (GDPR), because the British government feels “proud of adopting that piece of EU legislation”.4

Diversifying Data With Artificial Intelligence And Blockchain Technology

An impressive feature of Artificial Intelligence (A.I.) is the technology’s ability to provide computational power to create cognition in machines. Yet A.I. critics today have become concerned that many artificial intelligence projects are centrally controlled and therefore producing "Narrow A.I." Unlike human cognition, narrow A.I. is not conscious or driven by emotion. Rather, narrow A.I. operates within a pre-determined, pre-defined range, even if it appears to be much more sophisticated than that. Virtual assistants like Google’s Siri and Amazon’s Alexa exhibit examples of narrow A.I. While these A.I.-based systems are able to communicate with users and answer questions, these machines are nowhere close to having human-like intelligence.

Backdoor in Popular JavaScript Library Set to Steal Cryptocurrency

A JavaScript library that scores over two million downloads every week has been injected with malicious code for stealing coins from a cryptocurrency wallet. The affected package is Event-Stream, built to simplify working with Node.js streaming modules and it is available through the npmjs.com repository. The injected code tries to steal the bitcoins in the wallet and then attempts to connect to copayapi.host and to the IP address 111.90.151.134 in Malaysia. The Event-Stream library continues to be available from right9ctrl via the npm manager but it does not present any risk. It appears that the rogue developer pushed an update to version 4.0.1 two months ago without the malicious code. Users on Github say that right9ctrl did this in a bid to hide their tracks, as most developers would tie their projects to a major version of the library but not update explicitly to it. This way, the backdoor would still be present in their projects but the latest revision of the package is clean.

---

2 House of Commons Library - Brexit and data protection - By John Woodhouse and Arabella Lang p.8
3 https://www.information-age.com/gdpr-and-brexit-123476453/
Impact of GDPR on Biometric Systems
by Paul Guckian – Lead Software Developer at Delaney Biometrics

Background
It is worth revisiting the meaning of “data”, under the Data Protection Act, which means information that is:

- a) being processed by means of equipment operating automatically in response to instructions given for that purpose,
- b) recorded with the intention that it should be processed by means of such equipment,
- c) recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
- d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
- e) recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Therefore, raw images of biometric data is “personal data” by the definitions of the Act. Raw biometric data may also meet the definition of “sensitive data” under the Act as it can reveal the racial or ethnic origin or even the health status of the user e.g. facial recognition would usually involve sensitive data as it reveals race for example. Of course, additional security controls are required for sensitive data under the Act. The proposed Model can guarantee, thanks to the use of the described Blockchain, data integrity through its structure which uses hash functions and digital signatures. Moreover the data sharing permits to the parts involved to trust each other and to hold their own copy of Blockchain, in such a way that every malevolent action of a node or a hacker can be easily identified and opposed. The model also guarantees transparency and privacy, because the data will be shared between all the parts involved even if they are encrypted, so if for any reason a bank needs to read a certain transaction it should only ask for the key to that single transaction to the affected banks or the EBA. Finally, a legal validity of the model could be recognized because, as we just said, data stored in the Blockchain must be digitally signed by the EBA or the banks involved in the transactions, so this data can't be disavowed. The complete report of our study is available on our website, www.gcsec.org, in reserved area “Publication”.

What is biometric data?

We should consider the two different kinds of “biometric” data which may be used:

**#1 Biometric images** are the raw picture of the biometric data (e.g. photo, fingerprint image), and is clearly personal data covered by the GDPR legislation. It can be readily encrypted to offer protection in storage or transit. This is the primary storage (along with templates) used by police and immigration systems, which can create confusion with the alternative approach used by commercial biometric systems.

**#2 Biometric templates** are hash values (same as password hash) representing the biometric patterns in numerical format. In itself, it is not normally considered “personal identifiable information” as it is a one-way hash and cannot in itself be “reverse engineered” to identify the user. This is the most common approach used by commercial biometric systems, which usually discard images to create a “vendor lock” effect when selling their system and prevents migration to alternative systems.

But there are two data scenarios to be careful of when considering the impact of GDPR. Firstly, if another system has the raw data to re-create the template, and the data can be matched via an index, then it may meet the definition of personal identifiable information. Secondly, all systems have to process a raw biometric image in memory to create or verify the biometric template so some ‘personal identifiable information’ is involved in all cases. Most commercial systems operate using this approach.

Impact of GDPR legislation

There remains a great deal of ‘best practice’ to be defined around the impact of GDPR and biometrics, and there still remains many conflicting views about the interpretation of the legislation with many ‘consultants’ erring on the side of caution. In relation to biometric data, the main principals of the new GDPR legislation are:

1. Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

   Biometrics is no different to other forms of sensitive data, you must obtain permission to process the data. In most cases, biometric enrolment requires the users to comply with the enrolment process. Passive surveillance using biometrics is obviously an area where consent needs to be clearly communicated, probably via signage or other means.

2. Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

   Biometrics is the same as any other sensitive data in this regard.

3. Data minimization: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

   There are clear business examples of where biometrics has exceeded the benefits of alternative authentication. Some examples include:
   - Construction timesheets are up to 10% more accurate when biometric
systems are used as it reduces buddy punching, ghost workers, and human error.

- Gym biometric access control reduce revenue loss by up to 5% for example, as it reduces card or PIN sharing. Ironically, the issue is highest in the lowest cost operators.

Therefore, business legitimately assess that biometric authentication is necessary to protect their commercial interests and staff safety matters, enabling these two sectors to operate on narrow profit margins. Other authentication options simply don’t provide a genuine link to the system user and are open to easier and possibly greater misuse or fraud. Storage of raw biometric images may be considered excessive or even unnecessary, when biometric ‘templates’ would have sufficed, so careful consideration needs to be given to the storage approach used.

4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date. Biometrics is the same as any other sensitive data in this regard.

5. Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

One point which is often raised is that biometric data must begin in a raw format before it is converted into a ‘biometric template’. Clearly, some raw image processing is necessary to turn the image into a template. Higher security biometric sensors carry out encryption and/or template creation on board the hardware module and also offer hardware identification controls to restrict connection of unauthorised hardware thereby managing the risk effectively. In terms of risk assessment, the same risk scenario exists with key logging for example, in that the system input data can be intercepted before it actually reaches the system. This is particularly relevant in the area of cybersecurity, so therefore a similar risk assessment approach may be taken with biometric inputs. At the point a user is presenting themselves to a biometric system, they are consenting to do so, which makes its similar to entering data on a web page.

6. Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Biometrics is the same as any other sensitive data in this regard.

7. Accountability: The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.

Biometrics is the same as any other sensitive data in this regard.

Impact on Biometric Systems

The benefits of biometric authentication are significant for many organisations, as it is both a convenient and secure form of individual authentication. Biometrics are the only authentication mechanism which truly links actual users (rather than their security identity) to their specific actions. It is also the only authentication method to offer true deduplication of user records, hence its use in voting systems. Native biometric data has the same ‘personal identifiable information’ data classification as any other personal information such as Name, Date of Birth etc., and in many cases comes under sensitive data it would identify the race or ethnic origin of the person.

Some of the arguments against biometric data is that it cannot be changed, but this is similar to ‘Date of Birth’ and other sensitive personal data in this regard. Biometric templates are ‘hash values’ and don’t directly identify users, and these stored values can be changed by using an alternative algorithm approach. Indeed some system that detect an exact ‘replay’ of biometric data reject the input as its is statistically unlikely that you would have a mathematically perfect match.

The use of biometrics may be quoted as “excessive” or “unnecessary” by those objecting to its use. If construction timesheets are up to 10% more accurate when biometric systems are used and gym biometric access control reduce revenue loss by up to 5-10%, then the use of biometric systems has real and genuine value to businesses.
This enables these two sectors to operate on very narrow profit margins. Business legitimately assess that biometric authentication are necessary to protect their interests, as other options simply don’t provide a genuine link to the system user, are less convenient and potentially more open to fraud. In biometric systems, the ‘personal identifiable data’ is being processed when the biometric data (e.g. fingerprint) is captured by the scanner to when it’s converted into a template or used for authentication seconds later. Except in the case of passive surveillance, raw biometric data has to be ‘offered’ by the end user so therefore by definition has their consent. During the first phase, the raw biometric image is processed by the scanner and within seconds it is using the biometric template (secure hash value).

The data is processed like any other data between the client and server thereafter, such as the use of web browsers. In this regard, it’s no different than typing your date of birth or name on a web page before it’s securely processed by a web application. There is a moment when the data is exposed on the screen before it is then secured.

Conclusions

The use of biometric data is a well established mature authentication mechanism. It cannot be considered ‘excessive’, as there are very sensible and commercial reasons to require its use (de-duplication, anti-fraud, accuracy, convenience).

Just as your bank requires a 3-5 year address history to identify you and detect fraud, a biometric system may be a legitimate requirement for customers or internal users. If an alternative authentication is offered, then this can mitigate the feeling of ‘compulsory’ biometrics, but this can quickly undermine the security of the biometric system, the more secure approach is multi-factor biometric authentication.

Passive biometrics is probably the one area that is affected, but the millions of CCTV cameras in use in the UK will need to consider the impact of GDPR. In some sectors like pubs, CCTV is a licensing requirement, so it will take some time for the legislative impact to be established in case law and fully understood consistently.

Biometric data can be a sensitive subject for some end users. There are links with police and immigration systems which can generate emotive meanings for end users. However in law, biometric data with regards to GDPR legislation, is just another form of (sensitive) data. The ICO has issued specific guidance on the use of biometrics for children for example.

Biometric enrolment should be subject to the same consents and approvals as any other sensitive data. Raw biometric data is personal data in the case of risk assessment categorisation, and may be sensitive data. Biometric templates may or may not be personal data depending on system design.

Therefore, the design of the system needs to be carefully understood to correctly assess the impact.

The use of biometric data is not directly threatened by the GDPR legislation, and any organisation which designs its procedures to comply with the GDPR legislation should include ‘biometric data’ in its risk assessment in the same manner as other sensitive data.
A tsunami of reports, research & updates about the General Data Protection Regulation (GDPR) compliance before and post May deadline still seems insufficient to handle the compliance efforts with this regulation. One of the latest that hit my inbox just few weeks ago sounds like this:

A new research report made by TrustArc, benchmarks the GDPR compliance status post May 25th deadline of 600 US, UK and other EU companies. “...It provides information as to their GDPR compliance approaches, top compliance challenges and post-deadline needs, among other issues. Some of the key takeaways, are:

- Only 20% of companies have fully completed their GDPR implementations;
- Companies are most compliant with updating policies and procedures and cookie consent management, and least compliant with vendor risk management and international data transfer;
- 50% of the companies will seek a GDPR compliance validation from an independent firm.

The fact that a company can be compliant with updating policies and procedures but less compliant with vendor risk management and international data transfer doesn’t sound totally right.

Yes, the policies are part of the GDPR road map compliance, but they should, at their best, mirror and reflect among others how the vendor risk is managed all the way through international data transfer. And yet, businesses had two years of transition period in order to implement the GDPR within their processes.

But it was not a matter of time and even a matter of not being familiar at all with data protection laws.

The real issue with this regulation is that for the first time we’re facing on a large scale the missing culture within businesses and in the public sector as regarding to the way they treat and protect personal data.

And how important is the security of the information assets in our digital world.

And all this come out in the middle of a new wave of digital transformations such as AI, IoT, Blockchain and cryptocurrencies. Technologies that feed themselves with our data among other. We all know, and with GDPR we should know, that our identity, based upon our personal data, is directly related to everything we use and do from:

- Financial & legal services
- Healthcare
- Voting
- Property ownership (physical and intellectual property)
- Communication
- Entertainment
- Travel, to
- Security features and measures – some of them already based on personal data (mostly on biometric data such as fingerprint, face and voice recognition, heart beatings to mention few).

Thus, the way these data elements are being used and the services that all these technologies are promising to offer are very important to the economy and to the wellbeing of our society. And here is where GDPR places itself. There might be different ways to see and interpret GDPR, in the means of real applications and implications.
But a few basic considerations must be made which are unlikely to change for many years to come:

First, besides the mere legal meaning of General3 and Regulation4, the subject matter of GDPR is personal data and protection and within its articles we find in more detailed terms who, how, what, where, and when. The main areas being:

- Data subject rights;
- Accountability;
- Security;
- Processors, third parties and International data transfer;
- Higher sanctions -thought to be as a more cost-effective way of reducing the abuse of this right!

Second, the central reason of its implementation is to incorporate fundamental rights into EU legislative process. Specifically, the right of protection of personal data which is stated in Article 8 of the Charter of Fundamental Rights of European Union5. GDPR is far from perfect and with respect of its efficiency, it requires ten years practice in order to prove itself. And might be subject to changes, and, as often happens with any legal act, is open to interpretation. However, one thing will not change, at least for a long time and this is the fundamental right of protection of personal data.

Third, it aims to restore the trust in the digital and in the businesses, to promote innovation, enhance cyber security, and steer both the culture and the practical ways of evolving of our digital life and its security. Cyber security cannot be enhanced without a proper understanding of the relationship between security and other national (and international) imperatives such as privacy, transparency and technology. Having regard to the Cyber 2025 Model proposed by Windows, it can be said that GDPR places itself in the Peak scenario, which has as one of key characteristics: clear, effective government policies and standards6.

Fourth, GDPR is becoming a de facto standard around the world. Think only of the tech companies that treat customer data and have to be obeyed by any multinational that operates in Europe. But not only. It is leading the way to other countries outside the EU. The latest one being California which passed a sweeping consumer privacy law that might force significant changes on companies that deal in personal data – and especially those operating in the digital space. While the law, which is set to come into effect at the start of 2020, technically applies only to California residents, it will most likely have much broader implications. Most major companies that deal in consumer data, from retailers to cellular network providers to internet companies, have some Californian customers.

That will leave those companies with two main options: either reform their global data protection and data rights infrastructures to comply with California’s law, or institute a patchwork data regime in which Californians are treated one way and everyone else another. That last option can be more expensive for companies and could disgruntle non-Californian customers should they be given fewer data privacy options by the service provider. Indeed, similar questions about Americans’ data rights arose during Mark Zuckerberg’s congressional testimony in regard to Facebook’s compliance with EU GDPR. But, where to focus, being both personal data and cyber security among with developing cutting edge technologies the main topic of our agendas?

Compliance in general is a burden and bares real cost to the entire society.

And GDPR is not an exemption. As a matter of fact, any applied compliance within an organisation requires three essential things:

- Compliance Culture
- Ongoing Monitoring
- Team Efforts

Compliance culture: In recent news we read: “The Information Commissioner’s Office (ICO) has fined Lifecycle Marketing (Mother and Baby) Ltd, also known as Emma’s Diary, £140,000 for illegally collecting and selling personal information belonging to more than one million people.” There is everything but a compliance culture in this example. And yet, controversial behaviours from both companies and customers are part of the today debate. Here it’s a quote from Chris Rouland, founder and CEO of Bastille - “I see an opportunity to pay a premium for retaining my own data, or at least guaranteeing that my data is de-attributed from me,” he said, adding that he’d happily pay his fitness wearable provider another $1.99 (£1.33) a month not to sell his data somewhere else. As Geoff Mulgan - Chief Executive Officer at Nesta puts it in one his lectures at University College: ’Most people feel quite anxious when they discover just how much information they are leaving behind, and yet there’s a huge advantage to be gained from this collecting of data, the sharing of data, the cross-mining of data to offer people services in better ways, to reduce crime and so on. My guess is in the next 10 years we will need almost a new social contract around that data.’ For the moment we just had a legal basis of that contract - the GDPR.

Ongoing monitoring: - “A hacker broke into a few of Reddit’s systems and managed to access some user data, including some current email addresses and a 2007 database backup containing old salted and hashed passwords. Since then we’ve been conducting a painstaking investigation to figure out just what was accessed, and to improve our systems and processes to prevent this from happening again.” reads a data breach notification published by the company. What if a Data Protection Impact Assessment (DPIA) was made before, what if the investigation of what you already have would have helped to make the post investigation and hence the response plan less painful, more cost effective, more reliable and receptive? The ongoing monitoring of the systems and processes as a normal practice of the cyber resilience it is not an option anymore under GDPR. It’s mandatory. The players involved still underestimate the importance of both cyber security and personal data.

Sooner or later the waves of regulations will make the cyber security – which until now is looked as a mean to protect valuable assets and based upon principles – as a right and asset in its own. Or at least, in the near future we can except a more detailed and rule based cyber security strategy.

Team Efforts: - the fact is that even the big fails. Google recently removed 145 applications from the official Google Play store because they were found to carry malicious Windows executables inside. The type of infection “is a threat to the software supply chain, as compromising software developers has proven to be an effective tactic for wide scale attacks".
So far, personal data as a digital asset and cyber security is still not going hand to hand. It is normal to ask why it’s missing the Information Commissioner’s Office from what it seems one of the most important alliance in UK cyber security strategy? And though the invitation to participate was open to other organisations to join the alliance, the fact that the Data Protection Authority was missing on the first call speaks volumes. The truth is that the link between personal data as a digital asset and not only compliance burden under GDPR (or national privacy bills) and cyber security as a mean to protect those assets is dimly perceived even on top levels.

In conclusion, GDPR speaks to all of us. The challenges create opportunities. GDPR is inviting to develop creative ways to balance conflicting issues and guarantee the protection of personal data as a human right. If it is true, that is tremendous value to be unlocked in applying digital technology to new customises services and more in general to our lives, it is also true that with the nascent technologies that are emerging now, we can’t dismiss the serious ethical issues surrounding technologies such as artificial intelligence or genomics to mention few. If we’ve spent the last few decades learning how to move fast, over the next few decades we’re going to have to relearn how to go slow again.

Or maybe the one way to move forward is to restore simplicity and efficiency. And we cannot think in silos either. Everything is interconnected, so are the interests involved, the players, the regulations, the data and the security.

We can not afford to go back but we have the responsibility to make right and responsible choices now, in order to shape a better future of our digital as a real digital life. There is more in being compliant and it is not a kind of decision-making which requires only a cost-benefit analysis. Who hasn’t seen the personal data asset that needs to be protected or who has abused of it, now it’s the time of making things right.

So, think of GDPR not as a compliance burden, but as game changer, and to use it as aid to a more coherent and ethical progress in building new technologies and doing new businesses taking into consideration its core principles:

- security of personal data,
- responsibility and accountability on top of the businesses, but also on top of us as individuals
- its relationship with other core principles of our society and ever evolving of new technologies.