Coding for Privacy: An Agile Approach to Address Dynamic Privacy and Data Protection Requirements.

Kiran Bommareddy

Introduction

Over 100 nations have laws and regulations to protect personal data and privacy.[1] This strong global trend to adopt such rules is fueled by the increasing political, economic, and social importance of personal data, exacerbated by constant news of security breaches and the growing understanding by world citizens of the harmful effects of personal data loss. As a result, many countries have adopted or are formulating regulations and laws. This phenomenon translates into developing and deploying secure products and services at a faster pace.

While there are common foundations to protection of privacy and personal data, discussed further below, it may manifest in different ways around the world. For example, the United States established sectoral privacy laws[2], sometimes focused on harm[3], European regulators emphasized the human rights aspects of privacy[4], and Asian countries have tended to approach privacy protection as a global trade issue[5]. Organizations that operate globally must produce products, solutions, and services that meet regulatory requirements of these diverse markets. By understanding different laws and regulations in principle and their commonalities, it is possible to manage these global requirements by establishing a single global privacy and data protection policy outlining the necessary controls to protect personal data. The controls can then be mapped into the development and operational lifecycle of the products and solutions.

While privacy laws and regulations can guide an organization's global policies, they cannot solely define it. Organizations have to build the products and solutions with security and privacy in mind from the beginning of the product design and development phase. A systematic engineering approach is beneficial for organizations to develop policies based on the organization's goals and appropriate government regulations. Security procedures, standards, guidelines, best practices, privacy rules and mechanisms can then be designed and implemented according to systems engineering methodologies, models and patterns.

Agile development techniques with integrated security and testing approaches can help embed privacy and security into the products from the start and continuously. Privacy requirements can

---

1 "DLA Piper's Data Protection Laws of the World." https://www.dlapiperdataprotection.com/. Accessed 10 Feb. 2019.

2 "Data protection in the United States - Practical Law - Thomson Reuters." 1 Oct. 2018, https://uk.practicallaw.thomsonreuters.com/6-502-0467. Accessed 10 Feb. 2019.

3 "Topic #4: The intersection between privacy, big data and competition." 20 Aug. 2018, https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0022-152095.pdf. Accessed 10 Feb. 2019.

4 "Data Protection | European Data Protection Supervisor." https://edps.europa.eu/data-protection/data-protection_en. Accessed 10 Feb. 2019.

5 "Balancing Data Protection and Free Flow." https://www.apec.org/Press/Features/2018/0319_ppd. Accessed 10 Feb. 2019.

change due to factors external to the organization, such as legal, consumer and regulatory developments. The product development projects must be able to incorporate new requirements at any point in the development and operational lifecycle. Agile processes can enable the teams to prioritize changing requirements and develop controls.

This paper is divided into three sections. The first section consists of foundational privacy principles and the current state of global data protection and privacy laws. It sets out the need for faster product delivery to comply with changing regulations and laws. Section two describes the two dominant product engineering methodologies, waterfall and Agile, and the selection of the Agile framework to deliver faster and more secure products. Additional steps to incorporate security and test into the Agile framework are discussed. The third section offers recommendations to improve security and privacy assessments, requirements engineering, and augment Agile process enhancements with privacy baselines and product release criteria.

Current Global Data Protection and Privacy Laws and Regulations

There are privacy and personal data protection laws that are actively enforced on almost every continent in the world. The following examples illustrate the broad reach of regulation. The General Data Protection Regulation (GDPR)[6] entered fully into force in 2018 in all member states of the European Union. The Unites States and Canada have multiple federal, state and provincial laws[7]. The EU-US Privacy Shield[8] sets forth the necessary adequate protection and safeguards to permit personal data transfers between the US and EU. Israel started enforcing the Protection of Privacy Regulations[9] which requires extensive information security requirements for all organizations based in Israel.

In Australia, there is various legislation related to data protection. Australia passed the Privacy amendment in 2016, introducing breach notification laws to the Privacy Act[10]. Elsewhere in the Asia-Pacific region, the China Cybersecurity Act[11] came into force in 2017, with emphasis on safety and security of personal data by service providers. In India, the Supreme Court declared privacy as a fundamental human right[12], paving the way to draft data protection and privacy regulation.[13]

---

6 "The Regulation - GDPR." https://eugdpr.org/the-regulation/. Accessed 10 Feb. 2019.

7 "A Comparative Analysis of Regulation in the US, the EU and Canada." http://www.avocatshorsquebec.org/site/fr/les-nouvelles/articles/302-privacy-at-the-crossroads-a-comparative-analysis-of-regulation-in-the-us-the-eu-and-canada.html. Accessed 10 Feb. 2019.

8 "Privacy Shield Program Overview." https://www.privacyshield.gov/Program-Overview. Accessed 10 Feb. 2019.

9 "Privacy Overview 2017 - DataGuidance." 1 Jan. 2018, https://www.dataguidance.com/privacy-overview-2017/. Accessed 10 Feb. 2019.

10 "Notifiable Data Breaches scheme| Office of ...." https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme. Accessed 10 Feb. 2019.

11 "Z7AS-WUMA: Law in China - DLA Piper Global Data Protection ...." https://archive.org/details/perma_cc_Z7AS-WUMA. Accessed 10 Feb. 2019.

12 "in the supreme court of india civil original jurisdiction versus." 24 Aug. 2017, https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf. Accessed 10 Feb. 2019.

13 "India's Supreme Court Upholds Right to Privacy as a Fundamental ...." 28 Aug. 2017, https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time. Accessed 10 Feb. 2019.

In South Africa, regulations are being drafted to supplement the protection of personal data Act 2013.[14] The Tunisian parliament approved data protection legislation in 2017[15] and Egypt approved a similar bill in August 2018[16]. In South America, the Argentina Data Protection Authority[17] issued new regulation, series of principles and rights to data subjects. In the Caribbean, the Cayman Islands, Jamaica, Trinidad and Tobago introduced and passed various data protection and cybercrime bills.[18]

In Russia, the new personal data violations laws will enforce actions against violations of data subject rights[19]. Moldova, Belarus and Ukraine also passed cybersecurity laws that are similar to Russia.[20]

Foundational Principles of Protection of Privacy and Personal Data

All these regulations and laws enforced in various countries impose numerous obligations on critical infrastructure manufacturers, hardware and software vendors and service providers. While the origins and reasons for data protection legislation in various countries may be different, they tend to have very similar intent and principles to protect personal data. All standards converge on primarily three principles – Transparency, Fairness and Accountability. All the organizations, service providers and equipment vendors deploying services across the globe should start building their products and solutions encompassing these data protection and privacy principles.[21]

The Fair Information Practices (FIPs)[22] were adopted in 1973. The FIPs were openness, individual access, individual participation, information management and accountability. The FIPs were incorporated in the 1974 US Privacy Act[23], which added three additional elements: collection limitation, use limitation and disclosure limitation. These eight foundational principles appear consistently in data protection and privacy laws around the world[24]. For example, the Organization for Economic Cooperation and Development (OECD) used these eight elements in

---

14 "Protection of Personal Information Act, 2013 - Department of Justice." http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf. Accessed 10 Feb. 2019.

15 "Tunisia ratifies Convention 108 and affirms commitment ... - Access Now." 17 May. 2017, https://www.accessnow.org/tunisia-ratifies-convention-108-affirms-commitment-protection-personal-data/. Accessed 10 Feb. 2019.

16 "DLA Piper's Data Protection Laws of the." https://www.dlapiperdataprotection.com/. Accessed 10 Feb. 2019.

17 "Missions and Duties - Agencia de Acceso a la ... - Argentina.gob." http://www.jus.gob.ar/datos-personales/english-version/missions-and-duties.aspx. Accessed 10 Feb. 2019.

18 "Privacy Overview 2017 - DataGuidance." 1 Jan. 2018, https://www.dataguidance.com/privacy-overview-2017/. Accessed 10 Feb. 2019.

19 "Russia - The Privacy, Data Protection and Cybersecurity Law Review ...." https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151296/russia. Accessed 10 Feb. 2019.

20 "Privacy Overview 2017 - DataGuidance." 1 Jan. 2018, https://www.dataguidance.com/privacy-overview-2017/. Accessed 10 Feb. 2019.

21 (The Privacy Engineer's Manifesto, 2014, pp. 42-50)

22 (Allen & Rotenberg, Privacy Law and Society , 2015, pp. 755-756)

23 (Allen & Rotenberg, Privacy Law and Society, 2015, pp. 756-757)

24 "A Brief Introduction to Fair Information Practices | World Privacy ...." 4 Jan. 2008, https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/. Accessed 10 Feb. 2019.

the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[25]. The OECD guidelines are collection limitation, data quality, purpose specification, use limitation, security, openness, individual participation and accountability.

Global organizational policy for product development

With an awareness of the required legal compliance for all the countries in which the organization operates, management has to make a decision on coming up with a single policy. While regulatory compliance is one important input to the single global organizational policy creation, there can be many other organizational and business objectives to consider. Customer expectations, ethics, security posture and market competitive advantage are some of those business objectives.

Privacy by Design[26] and Security by Design[27] are principles that the GDPR sets out as requirements for building products and services. In order to comply with the GDPR and similar regulations, organizations need to engineer privacy into products and services right from the idea inception and design phases. The organization's global privacy policy is an important tool in the privacy engineering process. Developers, testers, compliance teams and lawyers can use the same policy for expected behavior and accountability.

The ever-changing nature of privacy laws around the world creates a challenge in gathering privacy engineering requirements. Moreover, requirements are also driven by internal policies, industry standards, and importantly, customer expectations. Purpose, notice, choice, consent, data transfer, access, correction, deletion, security, minimization, proportionality, retention and accountability are some of the privacy requirements to be considered.[28] Many times, these requirements must be converted into actionable, technical requirements to be implemented in the products.

System Engineering Methodologies: Waterfall and Agile

All organizations have to select a product development methodology, in order to build better quality products, to improve collaboration, and to maintain standards compliance. The selection of product development methodology is fundamental in deciding the roles and responsibilities of the teams in the organization. The development methodology drives the products and services concept, requirements, development and test phases. The business and product teams must clearly capture and track requirements for the success of the product, irrespective of the selected development methodology.

---

25 "OECD Guidelines on the Protection of Privacy and Transborder Flows …."
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 10 Feb. 2019.

26 "Privacy by Design | General Data Protection Regulation (GDPR)." https://gdpr-info.eu/issues/privacy-by-design/. Accessed 10 Feb. 2019. Privacy by Design is an approach by which privacy principles are embedded in the system design and business practices.

27 "Art. 25 GDPR – Data protection by design and by default | General …." https://gdpr-info.eu/art-25-gdpr/. Accessed 10 Feb. 2019. Security by Design is a secure hardware and software development approach to reduce vulnerabilities and possible threats.

28 (The Privacy Engineer's Manifesto, 2014, pp. 99-104)

Waterfall and Agile methodologies are the two most commonly used software development methodologies. The waterfall method consists of a top-down approach, executed sequentially to a final rollout. The eight phases of the waterfall model are: Conception, Initiation, Analysis, Design, Construction, Testing, Implementation and Maintenance. This methodology is widely used in engineering projects that have a clear vision of the end result. The advantages of this model are detailed planning and clear understanding of the development path defined at the beginning of the project. The disadvantages are that it cannot adapt to changes midstream and that the testing phase starts only after the coding phase.[29]

The Agile model allows for delivery of software in smaller chunks, as a minimum viable product to meet customer needs. Customer feedback and software bugs are incorporated back into requirements for faster delivery of improved product. The project is broken down into smaller manageable tasks, called Sprints,[30] with software delivery every three to four weeks. The advantages of using the Agile approach are revisiting design as needed, frequent tested delivery and increased customer focus. The disadvantages are reliance on all the team members, and that the final product may end up being completely different from the initial product vision.

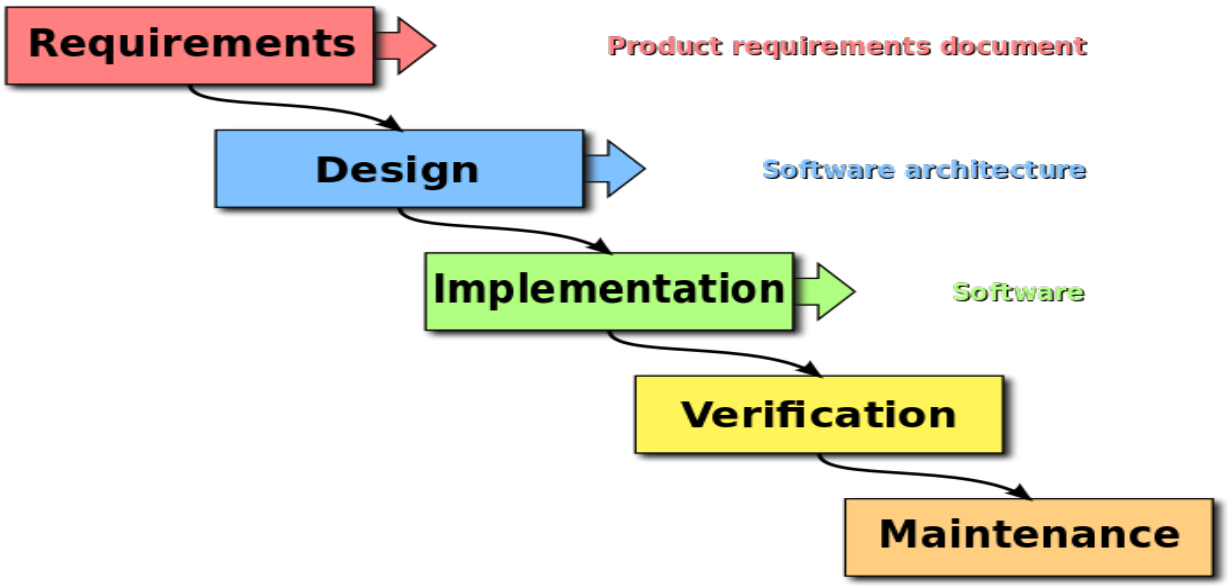

Figure 1. The unmodified "waterfall model". (Source: en.wikipedia.org)

29 "The Manager's Guide to Mixing Agile and Waterfall | Workfront." 6 Jun. 2016, https://www.workfront.com/resources/solve-the-pain-of-mixing-agile-and-waterfall. Accessed 10 Feb. 2019.

30 "Sprint Planning | Agile Alliance." https://www.agilealliance.org/glossary/sprint-planning/. Accessed 10 Feb. 2019.

There are many software development methods and approaches that are considered Agile and adhere to the values and principles of the Agile Manifesto[31]. The four values of the Agile Manifesto are: Individual and interactions over processes and tools, working software over comprehensive documentation, customer collaboration over contract negotiation, and responding to change over following a plan. Some of the Agile methods are Scrum, eXtreme Programming, lean Software Development, Kanban, Feature Driven Development, and Dynamic System Development Method.

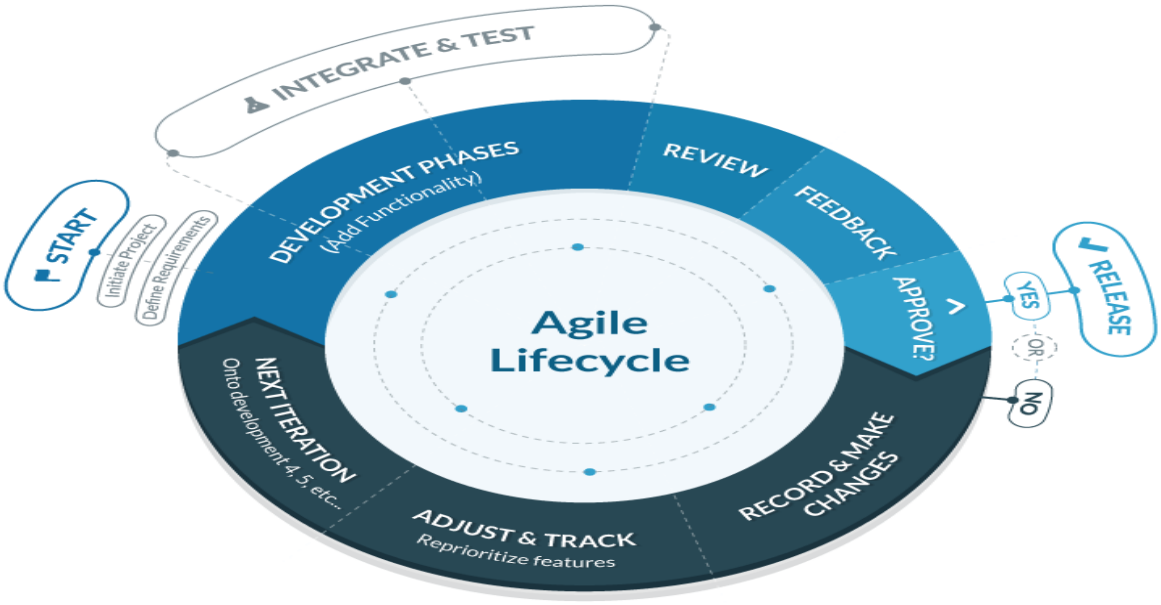

Figure 2. Agile development method (source: capterra.com)

Agile offers several advantages. It provides higher business value by allowing customers continuously to review the software as it is being developed. This continuous review and development allow the development team to adapt the product to suit the needs of end users better, increasing product use and value. The continuous product requirements that come from changing data protection and privacy laws can be inserted and evaluated in between the development cycles/Sprints.

31 "Principles behind the Agile Manifesto." https://agilemanifesto.org/principles.html. Accessed 10 Feb. 2019.

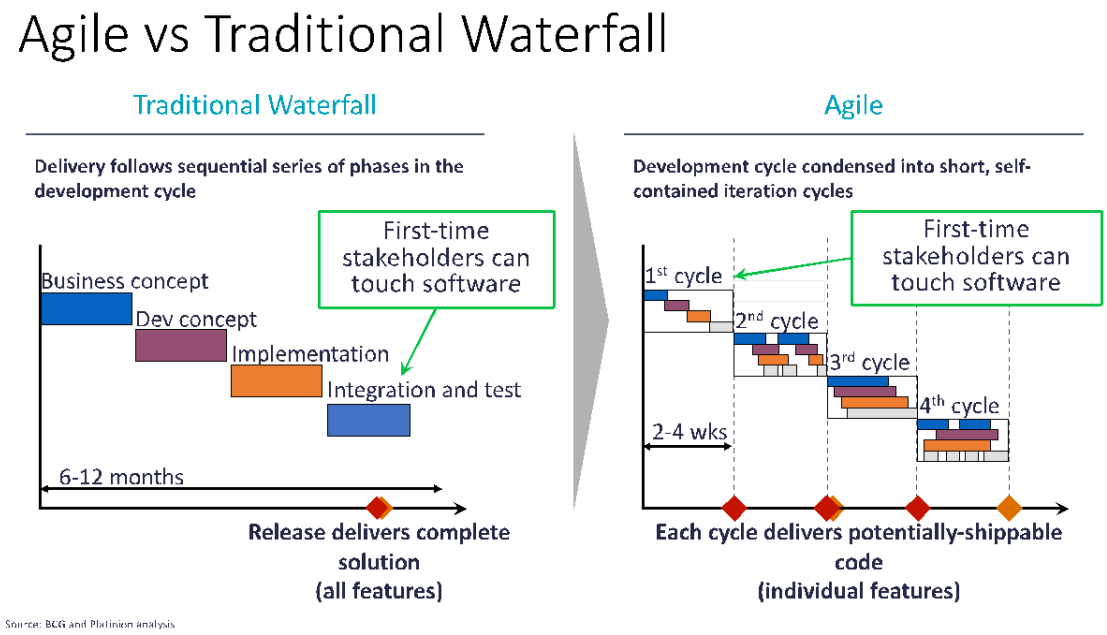

Figure 3. Comparison of Waterfall and Agile Methods

In view of changing product requirements coming from the international regulations and laws around the world, a product engineering methodology and lifecycle management process that can adopt change faster is needed. The Agile framework can accommodate the rapid change in requirements and circumstances arising from international and domestic regulations as well as customer needs.

Building Security Within the Agile Development Process

Security and privacy should complement each other and for privacy to be built into products and services, the security controls must be in place already. Building privacy into products and services without baseline security built into the product development process is an impossible task. Security Controls for Authentication, Authorization, Availability, Accountability, Encryption and Integrity are to be baked into the product development methodology from the initial project inception phase and continuously through every iteration.

Agile software development methods, by default, have not had security built into the framework. With the increasing threats to security in products and services, security is increasingly integrated into all Agile methods. Some of the proposed secure Agile methodologies[32] are Secure Scrum (S-Scrum) Secure Dynamic Systems Development Method (SDSDM) and security in eXtreme Programming.

32 "Integrating Security into Agile methodologies."
http://www.umsl.edu/~sauterv/analysis/F2015/Integrating%20Security%20into%20Agile%20methodologies.html.htm. Accessed 10 Feb. 2019.

Scrum is a popular framework, which consists of Scrum Teams and their associated roles, events, artifacts and rules. Scrum employs an iterative, incremental approach to optimize predictability and control risk. Transparency is achieved by having a common understanding of the processes among the people who are responsible for the outcome. Scrum teams review the scrum artifacts and progress at regular intervals to detect any undesirable variances. During the review, if there is a deviation beyond acceptable limits, the process or material must be adjusted. An early adjustment would minimize any further deviation and reduce the risk. Scrum describes Scrum Teams as self-organizing and cross-functional. Self-organizing teams decide their approach to accomplish their work, rather than being directed by anyone outside the team. Cross-functional teams have all skills required to accomplish the work without depending on anyone outside the team. This model of the team optimizes flexibility, creativity, and productivity. Artifacts defined by Scrum maximize transparency of key information, so that everybody has the same understanding of the artifact. Some of the Scrum artifacts are product backlog and Sprint backlog.

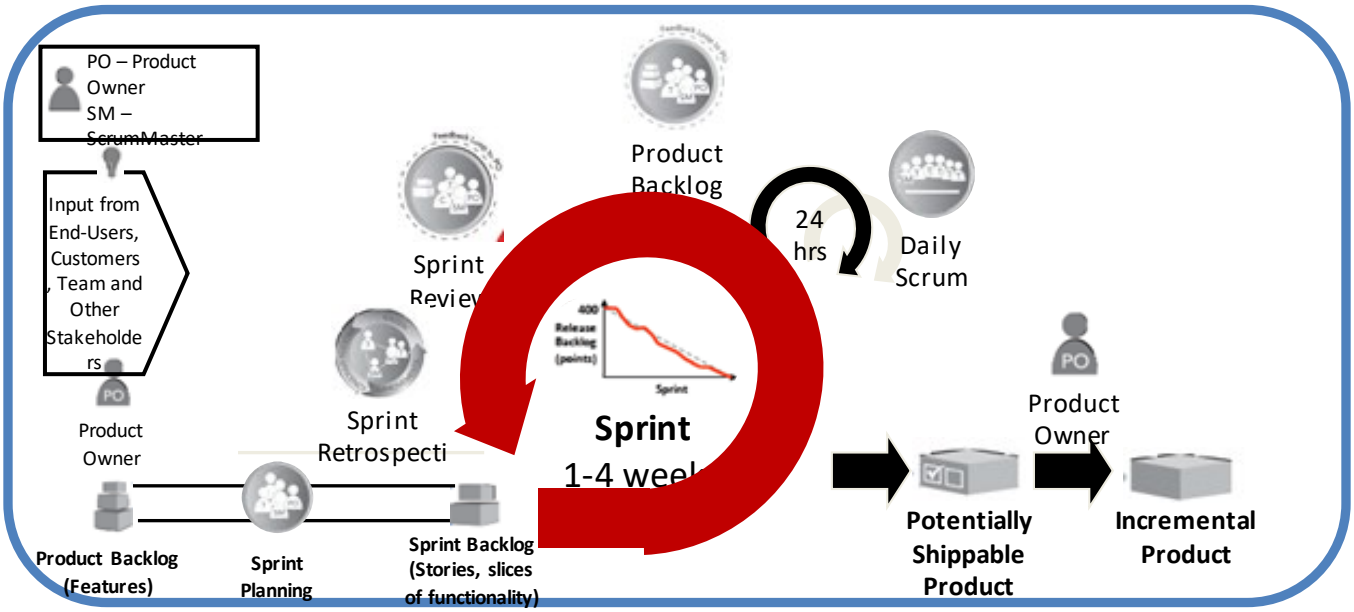

Figure 4. The Agile Scrum Framework (Reference source: snyxius)

There can be several ways to integrate security into the scrum process. Secure-Scrum, proposed by Pohl and Hof [33]is a variation of the Scrum framework, which focuses on the development of secure software throughout the Agile process. It adds four components that are linked to the existing scrum framework. A user story is a requirement expressed from end-user point of view. A label called S-Mark is used to mark the user stories that needs security. The S-Mark can contain one or more S-Tags. Each S-Tag contains the description of a security concern to help engineering team understand the problem and implement security principles. The S-Tag should be handled as long as the user story is marked with S-Mark.

In addition to integrating security in the Agile Scrum development method, security can be integrated in the testing phase of the Scrum[34]. Based on the proposal, a security test is done to test the developed security features in the same development environment with available tools. If any vulnerabilities are found, they are handled in the same Sprint towards releasing the software. The second security test is executed in the work environment. If any vulnerabilities are found, they are sent to Sprint backlog.

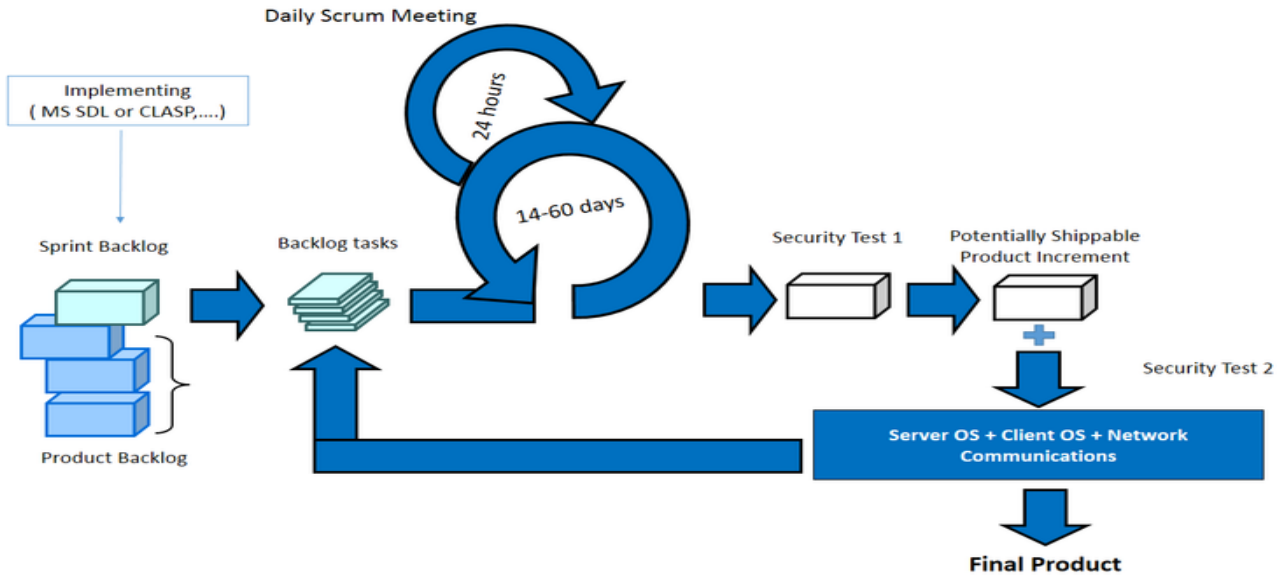

Figure 5. Scrum - security framework with test phases
(Source: Darwish & Megahed)

Product Requirements Analysis

During the product inception stage, requirements are gathered and listed in product backlog. There will be functional and non-functional requirements that goes into the product backlog, The Non-Functional requirements are elements that would be nice to have in the products, but are not mandatory. Unless the product being developed is a security product, security features tend to

33 "Secure Scrum: Development of Secure Software with Scrum - ThinkMind."
https://www.thinkmind.org/download.php?articleid=securware_2015_1_50_30099. Accessed 10 Feb. 2019.

34 "(PDF) A Security Testing Framework for Scrum based Projects." 30 May. 2016,
https://www.researchgate.net/publication/303679659_A_Security_Testing_Framework_for_Scrum_based_Projects. Accessed 10 Feb. 2019.

fall into the list of non-functional product requirements. The product requirements list, or "Product backlog" in Agile terms, can grow rapidly. As the non-functional requirements list grows, the development teams tend to ignore all the security and privacy requirements.

During the product inception phase, organizations should consider introducing security and privacy in the product design, based on the organizational policies, regulatory and legal compliance needs, as well as customer feedback. Recently, the laws and regulations started mandating the principles of security by design, privacy by design and privacy by default in the product design. These requirements force business and product owners to move the security, data protection and privacy requirements from the non-functional feature list to the functional feature list. The initial product backlog should contain all the design features that can help implement principles of security by design, privacy by design and privacy by default. The Business and product owners should set security and privacy baselines to include those principles in the products being developed. At the same time, automated tests need to be designed and developed to test the iterative product that will be released in every Sprint period.

Security Assessments and Privacy Impact Assessments

Security Assessments and Privacy Impact Assessments are to be done during the initial phase/Discovery phase of the product development. The assessments are carried out to identify the security, data protection and privacy gaps in the product design against the organization's security, privacy policies and regulatory compliance. The assessment reports will provide an opportunity for business and product owners to allocate enough resources to close the gaps or to decide to take the risks associated with deferring the security and privacy functions. If the assessments are done later in the development and implementation phases, fixing the security gaps can result in increased cost and delays. In addition, the patch work late in the implementation phase can introduce vulnerabilities that can be exploited by attackers. Security Assessment of the product should include the security objectives required by the product in terms of Confidentiality, Availability and Integrity. The following key tasks need to be done during the Security Assessment:

1. Identify the security requirements coming from regulations, laws, standards and customers.
2. Identify any certification and accreditation requirements.
3. Define common security controls needed by the product in all environments in which it can operate (private, hybrid and public cloud).
4. Perform threat modelling and identify threat surfaces to the product.
5. Identify security design and architecture to be used for the requirements specified.

In addition to Security assessments, the Privacy assessment should also be done in the initial phase of the product development. Privacy practices and tools need to be embedded in the initial design phase of the product, then constantly reviewed in every phase of product development. Privacy along with Security cannot be ad hoc at the later stage of product implementation. The domestic and international regulations and laws will change rapidly. Agile process needs to take care of additional new requirements in every Sprint. But, during initial Design phase, the business and product owners should consider all the current privacy regulations, policies and their compliance.

The Privacy Impact Assessment (PIA) consists of personal data scoping, privacy principles and the associated risks. The product software interacts with users in multiple way and so can be involved in collecting and processing personal data. PIA is an internal review of how the product being designed will collect and use personal data. Privacy data scoping, which is a part of PIA, involves full data lifecycle using the product, its flow and the controls needed to meet the organization's policies, regulatory compliance and customer expectations. The Privacy data scoping exercise should at least capture information about the product, system or software and how it related to FIPs in the following areas:[35]

1. Data – what data is involved and its sensitivity?
2. Purpose - How is the data processed and why?
3. Collection - means by which the data is being collections (human interface)
4. Notice - where is the notice presented to user and what is in the notice?
5. Consent - what kind of choice is given to the user?
6. Transfer - transfer of personal data to third parties or other systems in the organization? International transfer?
7. Access, Correction, deletion - how can the user control the data in terms of access/modify and deletion?
8. Security - Is personal data separated from other data? Is it secured with encryption and access control?
9. Minimization - Is the collection minimum to achieve the intended purpose?
10. Proportionality - Is the data processing proportional to the need and purpose?
11. Retention - Is there a plan defined and enforced for retaining or deletion of the collected date?
12. Third Parties - Any third-party software/components used in the product and is the relationship?
13. Accountability - Responsible parties defined?

Data gathering is done through data scoping mechanisms and analysis of that data results in determining how the personal data will be handled to conform to organizational policies and regulatory compliance, as well as the risks associated with handling the personal data. The risk assessment and the risk metrics used can differ from one organization to another. The main purpose of doing Privacy Impact Assessments in the initial product design phase is to understand the extent of personal data that will be collected, stored and created with the product about to be developed. The result is identifying the privacy controls to be incorporated in the product design and development. This assessment should be reviewed and updated while the product software is being changed with addition or deletion of features. In Agile framework, the PIA should be done, in addition to and along with the security assessment, in every Sprint.

Requirements Prioritization, Security and Privacy Baselines

The Security and Privacy Impact Assessments will contribute to the requirements list of the product development. Business and product owners have to make it a priority to insert security and privacy requirements in the initial product design. Based on the assessments done, the

35 "Privacy Impact Assessment (PIA) Guide - SEC.gov." https://www.sec.gov/about/privacy/piaguide.pdf. Accessed 10 Feb. 2019.

security and privacy requirements are graded with some degree of priority. The highest risk items take high priority and can be viewed as 'must have' in the initial product design and delivery. Irrespective of the development methodology that an organization selects, there should be a minimum set of security and privacy controls built for product release for regulatory compliance. In Agile methodology, the product evolution is continuous and the features will be added in every Sprint. But, the initial product release that meets minimum viable product for the market based on functional requirements, should also meet the full regulatory compliance in terms of privacy and security. Regulatory compliance for a product is not incremental.

Regulatory compliance is the primary reason for the non-functional requirements addition to the product design. But, organizational policies and customer feedback are also considered in the prioritization of the requirements. Privacy controls are built into the product on the foundations of data protection and security. Data protection, security and privacy requirements should be tied together during requirements analysis. Security requirements refers to functions needed to provide confidentiality, integrity and availability to protect all types of data. Privacy requirements are related to controlled processing and use of personal data.

A minimum set of data protection and privacy requirements must be included in the initial product design requirements list, with the view of having regulatory compliance. In Agile development method, these security and privacy baseline features must be designed and developed to be delivered in the initial product release. This product security and privacy baseline features should act as technical requirements to the product.

In Agile development methods, new features are added to the product in every iteration/Sprint. While the new features are added to the Sprint requirements, product owners and development teams should make sure that security and privacy baseline requirements remain intact. New features should be added on top of baseline security and privacy functionality.

Product Testing and Release Criteria

In Agile development methodology, the testing or validation phase is not elaborate and development teams themselves validate the developed features and move the product/service to release readiness. Development teams should write test cases that validate the features in every iteration of Agile development. In a similar way, the product security and privacy baseline features test cases must be written to use for validation. These security and privacy baseline test cases shall be validated in every Sprint cycle. This type of revalidation against baseline features tests ensures that the security and privacy baseline features are working as expected, even after the new Sprint feature development. In order to reduce time in this baseline testing, it is highly recommended to automate the test cases. Additional test cases will be developed in every Agile Sprint, and those test cases need to be tested manually before they are automated for the next Sprint. The Agile process will benefit from automating the bulk of security test cases.

Every product should meet strict criteria before it is released to customers. The Agile methodologies should be able to incorporate a gating process to check the readiness of the product security and privacy baselines. In the initial product release, all the product security and privacy baseline tests have to pass before the product is released to customer use. Development

should take the failed baseline test cases and fix them towards success. These mandatory readiness criteria will ensure the compliance of the release product. Subsequent Sprint releases can add security and privacy features to strengthen the initial release baseline features. The test failures of these additional security features need not hold a Sprint release, but it should trigger a feature readiness plan by the development team to fix it. The failed feature can go into the next Sprint and product backlogs to be looked into without delays. The product security and privacy readiness gate should be checked and verified by business and product owners, in addition to engineering project leaders. This process will help business leaders to understand the risk generated by allowing the Sprint release without full validation.

Avoiding Issues That Arise from Agile Practices

Agile development methods handle changing requirements and they will deliver the products early, and through continuous delivery. Agile methods deliver working software frequently, within a period of a few weeks to a few months. They incorporate iteration and continuous customer feedback to refine and deliver the product. With the frequently changing data protection and privacy laws around the world, Agile development frameworks will deliver the working software with speed and agility. Organizations are increasingly adopting Agile development frameworks to deliver products and services.

At the same time, continuous development and delivery of software products and related services can pose some new challenges. Modularity, temporality and capture[36] are some of the possible consequences from using Agile development. Software modularity is a result of a few ongoing changes in computing architectures. The first is the shift from standalone software products to Software-as-a-Service architecture. The client-server model moved most of the computing to the server side. The second change is the shift of computing power needs from client to server side. Server side scaling and performance needs gave rise to the need for large data centers with flexible resources. Services running in the cloud environment are aggregation of self-contained software modules. These software modules pass information and communicate using Application Programmable Interfaces. The software modules can be combined in different ways, creating different sets of services. Due to this nature of software modularity and ease of integration, the user's privacy is at risk. The users personal data will be exchanged and transferred between first and third parties. The service providers providing software as a service can add services from third parties to existing services to create a new service. This behavior will pose a challenge to user privacy in terms of who is in control and responsible for user privacy.

Agile programming practices allow developers across services to constantly tweak, remove, or add new features using continuous development loops. Changes to the service features happen regularly. These functional changes can result in an unceasing change in the relationship between the user and the services. A privacy principle, such as informed consent, can run into time limits due to the temporary relationships, and raise the question of when it is necessary once again to request informed consent[37].

---

[36] (Gurses & Van Hoboken, Privacy after the Agile Turn, 2018, pp. 579-601)

[37] For example, a company is hosting a social networking site where people can come together and chat. The service can be extended to include a feature for individuals to call each other. The service can be extended further with a

Agile development practices employ end users' activities and behaviors as feedback loops to optimize and deliver better solutions. In this process, organizations capture users' personal data and behavioral information that will be stored, analyzed and used in the process of offering better services. Development teams should take precautions on the selection of tools embedded in the software design and development to capture user activity. [38]

Conclusion

The constant changes in global privacy and data protection laws, organizational goals and customer expectations will force the product vendors and service providers to adopt strategies and methodologies that can enable them to deliver the products and services faster. Agile development methodologies are a natural fit to handle software product delivery at a faster pace, but initial frameworks lacked steps to include security and to protect privacy sufficiently. Due to the increased importance of incorporating security from product inception, various approaches are proposed by the engineering community to add security in Agile methodologies. Secure scrum is one such technique used to provide additional steps in the Agile process to add security. To start with, organizations have to select a secure Agile methodology of their choice. The selected development methodology has to be supported by product management steps. In order to provide regulatory compliance and market differentiation, security and privacy should be built into the initial product design. Thorough security and privacy impact assessments can drive product requirement lists with mandatory secure features, forming a security baseline. The development teams should incorporate these product security baselines in the initial design and move towards product development. Product release criteria based on successful security and privacy tests will enable the release of a product that can pass regulatory compliance and minimize business risk. It is recommended that the data scoping, classification and data flow assessments are done in every Sprint iteration of the product development. As the product changes in every Agile Sprint, the minimum security baseline requirements and release criteria should keep the security and privacy embedded in the product.

Works Cited

History: The Agile Manifesto, agilemanifesto.org/principles.html.

Project Management: Tools & Techniques, Personal Growth,

www.umsl.edu/~sauterv/analysis/F2015/Integrating Security into Agile methodologies.html.htm.

---

feature for exchanging payments. The company needs to understand the limits of the user's informed consent and to have a mechanism for revisiting and seeking additional consent, as needed.

[38] For example, engineering team may want to capture end user mouse movements to get feedback on a new feature. Based on the feedback, the development team can decide on the roll out of the feature. After the feature evaluation, the same mouse movements data can be used in conjunction to authentication mechanism using users behavior analysis. (Gurses & Van Hoboken, Privacy after the Agile Turn, 2018, pp. 595-596)

Allen, Anita L., et al. *Privacy Law and Society*. West Academic Publishing, 2016.

"Art. 25 GDPR – Data Protection by Design and by Default." *General Data Protection Regulation (GDPR)*, gdpr-info.eu/art-25-gdpr.

"Asia-Pacific Economic Cooperation." *Asia-Pacific Economic Cooperation*, www.apec.org/Press/Features/2018/0319_ppd.

"A Brief Introduction to Fair Information Practices." *Blog*, www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

Christoph Pohl, Hans-Joachim Hof. "Secure Scrum: Development of Secure Software with Scrum - Semantic Scholar." *Undefined*, 1 Jan. 1970, www.semanticscholar.org/paper/Secure-Scrum:-Development-of-Secure-Software-with-Pohl-Hof/ece4559a2c0b15aa8fe57297482a22a961bc4ccf.

"Compare Data Protection Laws around the World." *DLA Piper Global Data Protection Laws of the World - World Map*, www.dlapiperdataprotection.com/index.html.

Dennedy, Michelle, et al. *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. Apress, 2014.

Department. "Notifiable Data Breaches Scheme - Office of the Australian Information Commissioner (OAIC)." *OAIC*, Office of the Australian Information Commissioner, 2 Nov. 2018, www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

"Digital Economy." *Estadísticas - OECD*, www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

"GDPR Key Changes." *Key Changes with the General Data Protection Regulation – EUGDPR*, eugdpr.org/the-regulation/.

Gurses, Seda, and Joris Vredy Jan Van Hoboken. "Privacy after the Agile Turn." 2017, doi:10.31235/osf.io/9gy73.

Hébert, Jessica Joly. "Privacy at the Crossroads: A Comparative Analysis of Regulation in the US, the EU and Canada." *Association Des Avocats Hors Québec*, www.avocatshorsquebec.org/site/fr/les-nouvelles/articles/302-privacy-at-the-crossroads-a-comparative-analysis-of-regulation-in-the-us-the-eu-and-canada.html.

Kennedy, John B., and Paul M. Schwartz. *Second Annual Institute on Privacy Law: Strategies for Legal Compliance in a High-Tech & Changing Regulatory Environment, Summer 2001*. Practising Law Institute, 2001.

"The Manager's Guide to Mixing Agile and Waterfall." *Workfront*, 1 Jan. 3902, www.workfront.com/resources/solve-the-pain-of-mixing-agile-and-waterfall.

"Ministerio De Justicia y Derechos Humanos, Presidencia De La Nación." *Tipos y Modalidades De Violencia - Ministerio De Justicia y Derechos Humanos | Presidencia De La Nación*, www.jus.gob.ar/datos-personales/english-version/missions-and-duties.aspx.

Panday, Jyoti. "India's Supreme Court Upholds Right to Privacy as a Fundamental Right-and It's About Time." *Electronic Frontier Foundation*, 11 Oct. 2017, www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time.

"Practical Law." *Practical Law UK Signon*, uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default).

"Privacy Overview 2017." *DataGuidance*, 22 May 2018, www.dataguidance.com/privacy-overview-2017/.

"Privacy Shield Overview." *Ireland - Trade Agreements | Privacy Shield*, www.privacyshield.gov/Program-Overview.

"Privacy by Design." *General Data Protection Regulation (GDPR)*, gdpr-info.eu/issues/privacy-by-design.

Ramadan, Nagy, and Ihab Mohamed. "A Security Testing Framework for Scrum Based Projects." *International Journal of Computer Applications*, vol. 138, no. 7, 2016, pp. 12–17., doi:10.5120/ijca2016908928.

"Russia - The Privacy, Data Protection and Cybersecurity Law Review - Edition 4." *The Law Reviews*, thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151296/russia.

"SEC Web Site Privacy and Security Policy." *SEC Emblem*, 12 May 2017, www.sec.gov/privacy.htm.

Smith, John. "Data Protection." *European Data Protection Supervisor*, 11 Nov. 2016, edps.europa.eu/data-protection/data-protection_en.

"Sprint Planning." *Agile Alliance*, 13 June 2018, www.agilealliance.org/glossary/sprint-planning/.

"Tunisia Ratifies Convention 108 and Affirms Commitment to the Protection of Personal Data." *Access Now*, 17 May 2017, www.accessnow.org/tunisia-ratifies-convention-108-affirms-commitment-protection-personal-data/.

"Z7AS-WUMA: Law in China - DLA Piper Global Data Protection... : Free Download, Borrow, and Streaming." *Full Text of "Passing"*, London : F. Warne ; New York : Scribner, Welford, and Armstrong, archive.org/details/perma_cc_Z7AS-WUMA.

"JUSTICE K S PUTTASWAMY (RETD.), AND ANR. VERSUS UNION OF INDIA AND ORS." *Https://Www.sci.gov.in*, Https://Www.sci.gov.in, 24 Aug. 2017, www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

"Protection of Personal Information Act, 2013." *Http://Www.justice.gov.za*, Http://Www.justice.gov.za, 2013, www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.