FEATURE

Complying With GDPR
An Agile Case Study

Designed to give European Union residents better privacy rights, the EU General Data Protection Regulation (GDPR) comes into force in May 2018. It will replace the Data Protection Directive (Directive 95/46/EC).[1] GDPR consists of 99 articles that outline regulations and 173 recitals that provide conceptual and legal context for the articles.[2] Applying to all organizations that offer goods or services within the European Union or monitor EU residents' personal data, it will be enforced even if the personal data processing occurs outside of Europe.[3] Therefore, any organization handling an EU citizen's personal information must comply with GDPR. Uncompliant organizations can be subject to fines of up to EU €20 million, or 4 percent of their annual turnover—whichever is greater.[4]

This article presents a case study of a smart bracelet that bears many of the privacy challenges of a typical Internet of Things (IoT) project. As the number of organizations that adopt faster development methodologies increases, aligning the efficiency of the Agile model[5] with GDPR compliance can be daunting without guidance. To address this, a novel privacy-tagging approach as described in this article can be used along with state-of-the-art Agile methodologies to fulfill all the requirements of GDPR for developers, simplify auditing for compliance officers and ensure data protection for end users.

GDPR and the Software Development Life Cycle

GDPR redesigns personal data protection with the understanding that processing personal data is beneficial to society and that it must be balanced with a person's fundamental rights and freedoms.[6]

The regulation places the responsibility of personal data protection on developers and expects that they will incorporate data protection into their applications by design at the technical and organizational levels.[7] Additionally, for personal data processing that may pose a risk to the rights of individuals, as may be the case for data collection associated with new technologies, a data protection

Mina Miri
Is an application security researcher at SD Elements/Security Compass. She is particularly attuned to the need for applications to have well-developed security characteristics. In her current position, she researches secure development techniques in various security and privacy contexts. She has recently presented an Agile framework for building GDPR requirements into the software development life cycle at the Open Web Application Security Project (OWASP) AppSec USA 2017 and published an article in the *IAPP Privacy Tech* on a tagging approach to protection impact assessments (PIAs) in Agile software development.

Farbod H. Foomany, Ph.D., CISSP
Is lead application security researcher at SD Elements/Security Compass. He has been involved in various academic research and industry projects in the areas of privacy and security in software development, secure design of enterprise applications (Java EE), signal processing and evaluation of various aspects of biometric identification. Foomany has published and presented his work on signal processing and security in several IEEE conferences and journals, crime science conferences and networks, the International Association of Privacy Professional (IAPP) conference, and OWASP AppSec Conferences.

Nathanael Mohammed
Is a technical writer at SD Elements/Security Compass. He specializes in communicating about technology, with a focus on security and privacy. He has recently been involved with projects concerning GDPR requirements in Agile software development and published an article on a tagging approach to PIAs in *IAPP Privacy Tech*.

impact assessment is mandatory. This assessment determines to what extent the data processing of these technologies may impact the individuals who use them.[8] Consequently, many IT organizations will have to reevaluate how they build software so they can integrate GDPR compliance into their applications' life cycles.

The software development life cycle (SDLC) is divided into the following six phases: requirements, design, development, testing, deployment and maintenance.[9] Various methodologies provide different approaches to the development of a software product. In older methodologies, such as the waterfall model, one phase completes before the other phase begins.[10] However, more than half of IT organizations today use the Agile model, which is more flexible and realistic.[11] As such, the chief challenge for software companies is to create a solution throughout the development and deployment phases that is GDPR compliant. Likewise, the challenge for privacy analysts is to evaluate and audit compliance with the regulation.

> "THE CHIEF CHALLENGE FOR SOFTWARE COMPANIES IS TO CREATE A SOLUTION THROUGHOUT THE DEVELOPMENT AND DEPLOYMENT PHASES THAT IS GDPR COMPLIANT."

Implementing a solution that facilitates how software developers comply with GDPR is not a simple matter. To address this challenge, a list of 16 requirements to formulate the stipulations of GDPR for software development has been created.[12] Similarly, with more emphasis on deployment and operation, the International Association of Privacy Professionals (IAPP) has provided information on 10 operational impacts of GDPR.[13] This article proposes a different approach to GDPR-compliant software development based on a tagging method.

A Tagging Initiative for Building Privacy Into Agile Methods

In an approach presented to the Privacy Symposium 2017 at IAPP Canada,[14] a tagging method in which GDPR's text is coded in a way that is similar to the qualitative research methods of open coding, axial coding and selective coding was proposed.[15] The tagging approach consists of the following steps:

1. Identify tags for each GDPR mandate, where tags capture and code the essence of the mandate.
2. Review, merge and classify tags.
3. Assign tags to available privacy and security controls.
4. Generate privacy and security tasks for tags with missing controls.
5. Map tasks to GDPR mandates through tags.

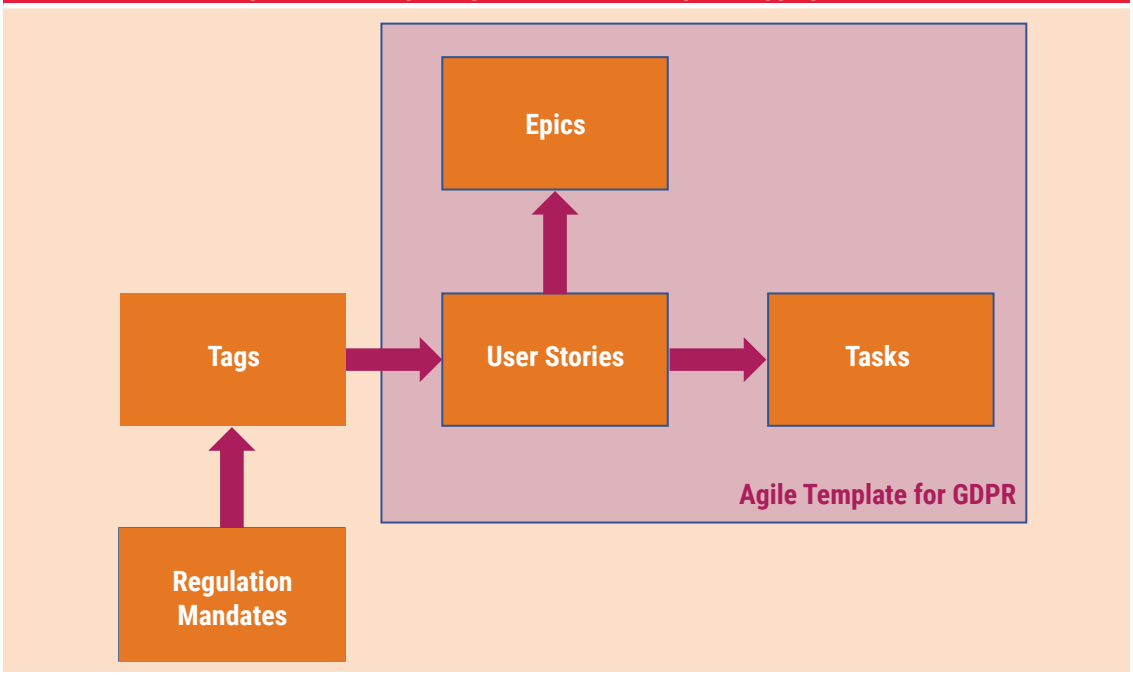
This approach allows for the generation of tasks based on tags, and the auditing of tasks related to each tag, which ensures that the requirements of mapped mandates are met.

Epics, user stories and tasks are essential to an Agile framework and need to be defined carefully to develop a group of activities that can take advantage of the efficiency of Agile sprints. Sprints are timeboxed units of development, such as two weeks, and are also called iterations. For an Agile GDPR framework, tags and articles can be used to define user stories, as demonstrated in the following figures. User stories express software requirements in a few short sentences. They are a simple description of a feature required by a person who is usually a user, customer or administrator. User stories often have the following structure:

As a <who>, I want <what> so that <why>.

User stories can then be organized into epics. An epic is a group of user stories with the same goal, and it is labeled to reflect that goal. An epic can usually be created for a group of user stories that fall under the same class of tags. **Figure 1** shows these elements, and how they are derived from tags.

Figure 1—Building an Agile Framework Using the Tagging Method



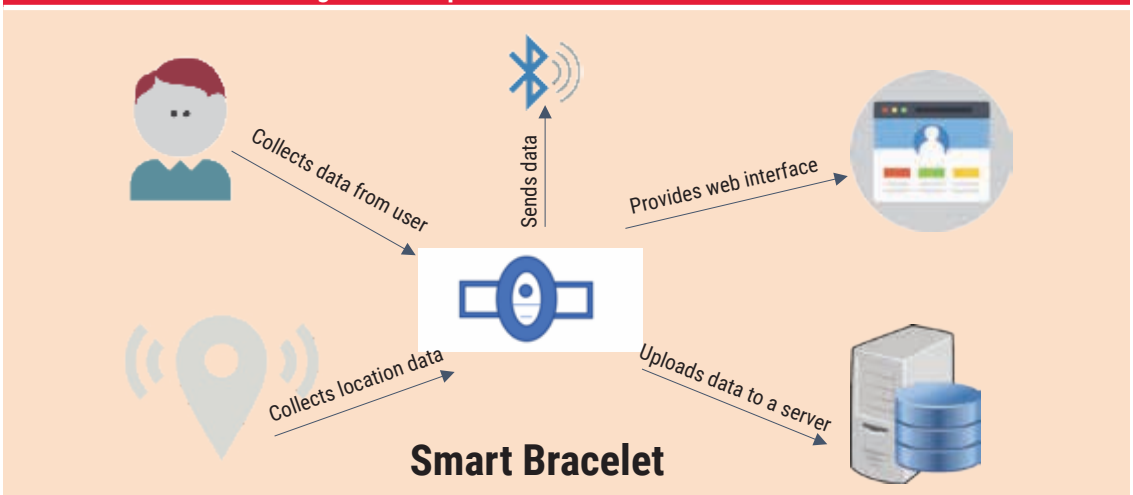
Case Study Project Description

A smart, wearable fitness-tracking device is developed as a bracelet and watch. This device collects personal data and health information from the user, including name, email address, height and weight. The device processes that information, transfers it to other devices via Bluetooth, and makes the wearer's location and ID available to a beacon or local transmitters. Some versions of this device also provide web applications for displaying information and further processing data. **Figure 2** shows the components of such a solution.

GDPR Tags, User Stories and Requirements

GDPR includes several articles and recitals that apply to devices that collect personal data. Using these mandates as a foundation, **figure 3** and **figure 4** were compiled. These figures demonstrate the results of tagging, article/recital mapping, user story writing and organizing of user stories into epics. In the case of the smart bracelet project, the GDPR requirements are clearly outlined, and the same strategy can be used for any project. **Figure 3** functions as a universal stepping stone for creating a complete Agile project by simply

Figure 2—Components of the Smart Device Solution



placing project-specific tasks under each user story. By using this strategy that weaves together the Agile methodology with GDPR compliance, any company developing any Agile project can track its GDPR compliance and prepare for compliance auditing and assessment.

Figure 3 provides the user stories for the core features required for the smart-bracelet project. Other user stories less central to the smart-device project are provided in **figure 4**. Based on the type of application being developed, the user stories in **figure 4** can also be relevant to other projects. The user stories in **figure 3** and **figure 4** are copyrighted by Security Compass 2018.

Figure 3—Core User Stories for a Similar/Typical Solution

Epic	Tags	User Story	Mandates
Achieve data protection	Data Protection: Pseudonymization	As a data custodian, the goal is to protect personal data so that one can provide privacy to data subjects and not be able to associate processed personal data with any specific individual.	Article 04/Recital 28 Article 04/Recital 29
Achieve data protection	Data Protection: Integrity/Accuracy	As a data custodian, the goal is to check/maintain/protect the integrity/accuracy of personal data on the system to ensure the accuracy of personal data.	Article 25/Recital 78 Article 32/Recital 83
Achieve data protection	Data Protection: Indirect Identification	As a user, the goal is to be able to provide/withdraw consent to/from the usage of data in identifiers that can be associated with individuals when combined with their personal data so that they cannot be identified indirectly by data in identifiers.	Article 04/Recital 30
Achieve data protection	Data Protection: Indirect Identification	As a user, the goal is to be able to receive customized services from an application without being directly/indirectly identified so that individuals can protect their privacy.	Article 04/Recital 30
Achieve personal data processing compliance	Compliance: Processing Ground: Consent	As a chief information security officer (CISO)/data protection officer (DPO), the goal is to access documents about the grounds for consent of processing personal data to determine compliancy with GDPR.	Article 06/Recital 40
Achieve personal data processing compliance	Compliance: Processing Ground: Consent	As a CISO/DPO, the goal is to know about processing activities and the type of data being collected so that stakeholders can determine the legal grounds for processing and collecting data types.	Article 06/Recital 40
Obtain consent for processing personal data	Consent: Consent Acquisition/ Withdrawal	As a user, the goal is to be able to provide/withdraw consent to/from processing personal data so that individuals can have control over how their personal data are processed.	Article 07/Recital 32 Article 07/Recital 33
Achieve transparent personal data processing	Transparency: Whole Program	As a user, the goal is to be able to easily access information about processing activities that involve individuals' personal data in clear and understandable language so they can exercise their right to view their processed personal data.	Article 12/Recital 58 Article 12/Recital 59
Achieve transparent personal data processing	Transparency: Whole Program	As a user, the goal is to receive information about personal data processing activities, including the purpose of processing and the safeguards used to protect individuals' personal data, so that they can exercise their right to information about why their personal data are processed and how they are protected.	Article 12/Recital 58 Article 12/Recital 59
Determine specific reasons for processing personal data	Purpose: Identification/ Limitation	As a user, the goal is to know the purpose of processing personal data and provide only the information necessary to fulfill that purpose so that individuals can prevent the unnecessary disclosure of their personal data to protect their privacy.	Article 05/Recital 39 Article 25/Recital 78
Achieve personal data processing compliance	Compliance: Processing Ground	As a CISO/DPO, the goal is to access documents about the grounds for processing personal data so that their compliancy with GDPR can be determined.	Article 06/Recital 40
Achieve personal data processing compliance	Compliance: Scope	As a CISO/DPO, the goal is to access documents about processing personal data so that whether the processing is consistent within the scope of GDPR can be determined.	Article 02/Recital 15 Article 02/Recital 19 Article 03/Recital 22 Article 03/Recital 23

Figure 3—Core User Stories for a Similar/Typical Solution *(cont.)*			
Epic	**Tags**	**User Story**	**Mandates**
Achieve personal data processing compliance	Compliance: Processing Ground: Sensitive Data/ Special Categories of Data	As a CISO/DPO, the goal is to access documents about the legal grounds for processing sensitive data (including health data and ethnic origin) so that their compliancy with GDPR can be determined.	Article 09/Recital 51 Article 09/Recital 52
Achieve personal data processing compliance	Compliance: Processing Ground: Legitimate Interest	As a CISO/DPO, the goal is to access documents about the grounds for legitimate interests for processing personal data so that their compliancy with GDPR can be determined.	Article 06/Recital 40 Article 06/Recital 47 Article 06/Recital 48 Article 06/Recital 49 Article 88/Recital 155
Achieve data protection	Data Protection: Sensitive Data/ Special Categories of Data	As a user, the goal is for sensitive data to be protected so that individuals can have privacy and safety.	Article 09/Recital 52
Carry out user notification	Notice: Notice	As a user, the goal is to get information about personal data processing activities during their operation so that individuals can exercise their right to know how their personal data are processed.	Article 12/Recital 60 Article 13/Recital 61 Article 14/Recital 62
Implement personal data information access	Access: Information	As a user, the goal is to be able to access information about personal data processing activities and have information about how individuals' data are processed so that they can decide whether they want to continue to use a system.	Article 15/Recital 63
Achieve data protection	Data Protection: Identification	As a data custodian, the goal is that only users with verified identities have access to personal data so that the privacy of users can be protected.	Article 15/Recital 64
Implement personal data information access	Access: Edit/Update	As a user, the goal is to be able to edit/update information in a system so that individuals can ensure the accuracy of and have control over their data.	Article 16/Recital 65
Implement personal data information access	Access: Removal/ Erasure	As a user, the goal is to be able to request personal data to be removed from a system under certain conditions so that individuals can limit how their data are used.	Article 16/Recital 65 Article 17/Recital 66
Implement personal data information access	Access: Restriction	As a user, the goal is to be able to send a request to stop processing activities on personal data under certain conditions so that individuals can exercise their right to restrict the processing of their personal data.	Article 18/Recital 67
Implement personal data information access	Access: Portability	As a user, the goal is to have/export processed personal data in a machine-readable format so that individuals can send them to other controllers.	Article 20/Recital 68
Achieve data protection	Data Protection: Confidentiality	As a data custodian, the goal is to take adequate security measures so that the confidentiality of user data can be protected.	Article 25/Recital 78 Article 32/Recital 83
Implement security risk reports	Risk Management: Security Risk Management	As an administrator, the goal is to have security reports so that plans for mitigating security risk can be developed.	Article32/Recital 83
Implement privacy risk reports	Risk Management: Privacy Risk Management	As an administrator, the goal is to have data-privacy risk reports so that plans for mitigating privacy risk can be developed.	Article 32/Recital 84
Perform limited data collection	Data Collection: Data Minimization	As a user, the goal is that the minimum amount of personal data are collected for processing activities so that individuals can prevent the unnecessary disclosure of their personal data.	Article 5/Recital 39 Article 25/Recital 78
Create and maintain processing records	Accountability: Documentation/ Demonstration	As a data custodian, the goal is to have a record of personal data processing and user activities, such as providing consent, so that these records can be provided to a CISO/DPO when needed.	Article 30/Recital 82
Create and maintain processing records	Accountability: Documentation/ Demonstration	As a CISO/DPO, the goal is to be able to see documents and records about personal data processing activities so that their compliancy with GDPR can be determined.	Article 30/Recital 82
Carry out data breach notifications	Auditing: Incident Reporting	As a supervisory authority, the goal is to be notified immediately after a data breach so that damage can be prevented and safety and security to data subjects can be assured.	Article 33/Recital 85 Article 33/Recital 88 Article 34/Recital 86 Article 34/Recital 87

Figure 3—Core User Stories for a Similar/Typical Solution *(cont.)*			
Epic	**Tags**	**User Story**	**Mandates**
Carry out data breach notifications	Auditing: Incident Reporting	As a user, the goal is to be notified immediately about the consequences of a data breach so that individuals can protect themselves from physical and financial damage.	Article 33/Recital 85 Article 33/Recital 88 Article 34/Recital 86 Article 34/Recital 87
Complete secure transfers of personal data	Compliance: Transfer	As a user, the goal is to have personal data protected during data-transfer processes so that individuals can ensure the safety and security of their data.	Article 44/Recital 101 Article 45/Recital 103 Article 46/Recital 107 Article 46/Recital 108 Article 47/Recital 111 Article 49/Recital 112 Article 49/Recital 113 Article 49/Recital 114
Complete secure transfers of personal data	Compliance: Transfer	As a CISO/DPO, the goal is to have information about transferring personal data, such as the types of data being transferred and the country receiving the data, so that the compliance requirements for transferring personal data can be determined.	Article 44/Recital 101 Article 45/Recital 103 Article 46/Recital 107 Article 46/Recital 108 Article 47/Recital 111 Article 49/Recital 112 Article 49/Recital 113 Article 49/Recital 114

Figure 4—Additional and Secondary User Stories for Other Solutions			
Epic	**Tags**	**User Story**	**Mandates**
Provide information about profiling processes	Profiling: Profiling	As a user, the goal is to be able to access information about the profiling process so that individuals can provide/withdraw their consent to/from being a part of profiling.	Article 03/Recital 24 Article 22/Recital 71
Carry out the evaluation of potential profiling activities	Profiling: Profiling	As a CISO/DPO, the goal is to be able to determine whether particular activities of a system qualify as profiling so that the lawfulness of those profiling activities can be evaluated.	Article 03/Recital 24 Article 22/Recital 71
Obtain consent for processing the personal data of children	Consent: Children	As a parent, the goal to be able to provide/withdraw consent to/from processing one's children's personal data so that parents can exercise their rights and control over the disclosure of their children's personal data.	Article 08/Recital 38
Provide special protection for children	Data Type/Services: Children	As a child, the goal is to have access to information about how personal data are processed in plain language so that children can understand the risk scenarios and data-protection safeguards for their personal data in a system.	Article 08/Recital 38
Achieve personal data processing compliance	Compliance: Processing Ground: Law	As a CISO/DPO, the goal is to access documents about the legal grounds for processing personal data so that their compliancy with GDPR can be determined.	Article 06/Recital 40
Achieve personal data processing compliance	Compliance: Processing Ground: Second Purpose	As a researcher, the goal is to use anonymized personal data for secondary purposes so that the content of the research cannot reveal the identity of any data subject.	Article 89/Recital 158 Article 89/Recital 159 Article 89/Recital 160
Achieve data protection	Data Protection: Archiving	As a data custodian, the goal is to be able to archive personal data lawfully with the appropriate safeguards so that the privacy and safety of archived data can be ensured.	Article 89/Recital 156

The next step is to assign tags to the privacy tasks of each phase and to then tie these tasks to user stories and their tags. **Figure 5** shows three privacy tasks that are grouped under a user story using the appropriate tag. Also shown in **figure 5** is a list of available privacy and security controls, such as those that are available in Application Security Requirements and Threat Management (ASRTM) solutions. These controls can be easily organized using tags so that protecting sensitive data is directly related to completing tasks in a repository of security controls.

Figure 5—Tying Tasks From Security Control Repositories to Tags and User Stories

Epic	Tag	User Story	Tasks
Achieve data protection	Data Protection: Sensitive Data	As a user, the goal is that sensitive data be protected so that individuals can have privacy and safety.	T244: Securely delete any unprotected sensitive data before a resource is released or shared. T139: Use secure channels to transmit protected health information on the Internet. T236: Test that the application encrypts protected health information on the Internet.

Conclusion

Integrating GDPR compliance with the SDLC is a major challenge for many IT organizations. This article presents a new approach to help development teams address the challenge in Agile environments. It presents an Agile GDPR template consisting of user stories, epics, relevant GDPR mandates and tags. The template and tags provide a list of GDPR mandates that apply to software/hardware development and deployment. This novel privacy-tagging approach can facilitate generating tasks and auditing for compliance so that GDPR compliance works in tandem with the efficiency of Agile development rather than against it.

Endnotes

1 EUGDPR.org, "GDPR Portal: Site Overview," *https://www.eugdpr.org/eugdpr.org.html*

2 SecureDataService, "EU General Data Protection Regulation (EU-GDPR)," *https://www.privacy-regulation.eu/en/index.htm*

3 SecureDataService, Article 3: Territorial Scope, *https://www.privacy-regulation.eu/en/3.htm*

4 SecureDataService, Article 83: General Conditions for Imposing Administrative Fines, *https://www.privacy-regulation.eu/en/83.htm*

5 Agile Alliance, "What is Agile Software Development?" *https://www.agilealliance.org/agile101/*

6 SecureDataService, Recital 4: EU GDPR, *https://www.privacy-regulation.eu/en/r4.htm*

7 SecureDataService, Article 25: Data Protection by Design and by Default, *https://www.privacy-regulation.eu/en/r425.htm*

8 SecureDataService, Article 25: Data Protection Impact Assessment, *https://www.privacy-regulation.eu/en/35.htm*

9 International Software Testing Qualifications Board Exam Certification, What Are the Software Development Life Cycle (SDLC) Phases? *http://istqbexamcertification.com/?s=What+are+the+software+development+life+cycle+phases%3F*

10 Half, R.; "Six Basic SDLC Methodologies: Which One Is Best?" 21 November 2017, *https://www.roberthalf.com/blog/salaries-and-skills/6-basic-sdlc-methodologies-which-one-is-best*

11 Computer Economics Inc., "Agile Development Use Increases, But Barriers Remain," January 2017, *www.computereconomics.com/article.cfm?id=2321*

12 Reid, G.; "How to Navigate the Software Development Life Cycle Under the GDPR," International Association of Privacy Professionals, 24 January 2017, *https://iapp.org/news/a/how-to-navigate-the-software-development-life-cycle-under-the-gdpr/*

13 Heimes, R., *et al.*; "Top 10 Operational Impacts of the GDPR," International Association of Privacy Professionals Privacy Symposium 2017, May 2017, *https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/*

14 Karbaliotis, C.; F. Foomany; *A Tagging Initiative for Building Privacy Into IoT Systems*, International Association of Privacy Professionals Privacy Symposium 2017, May 2017, *http://sforce.co/2h3MmdW*

15 Jaccard, J.; J. Jacoby; *Theory Construction and Model-Building Skills: A Practical Guide for Social Scientists*, Guilford Press, USA, 2010