An Agile Approach to GDPR Implementation within a Further Education College

Alex Harding

April 28, 2018

An Agile Approach to GDPR Implementation within a Further Education College.

Alex Harding
Runshaw College, Leyland, United Kingdom
University of Central Lancashire, Preston, United Kingdom
harding.a@runshaw.ac.uk

Abstract - **The General Data Protection Regulation sees a fundamental shift in the way in which data is handled, stored and distributed. Massive uncertainty exists due to the UKs proposed exit of the European Union and this has resulted in a complacent, ignorant attitude to the changes within a large number of UK businesses and public sector organizations.**

This paper explores the impact of the GDPR, it's relation and changes from the 1998 Data Protection Act and the intentions of the UK government. In addition, a proposal for a software solution to manage a number of aspects of Data Protection within a Further Education College is discussed along with a report on its implementation.

Discussion of the techniques and tools used to create the software solution and to manage the GDPR implementation using Agile Methodologies and Tools is featured.

Keywords - GDPR, General Data Protection Regulation, Information Asset Management, Data Flow, Data Subjects Rights, Agile, Jira

I. Introduction

April 26th 2016, saw the stopwatch start counting down towards enforcement of the EU's new Data Protection legislation., the General Data Protection Legislation (GDPR) [1].

> *"Time is running. On 24 May 2018 the General Data Protection Regulation of the EU (GDPR) will apply directly to processing activities of personal data... Those who try to create a different perception by denying these facts are putting in danger everyone who has to prepare for this new law in time until 24 May 24 2018." [2]*

The UK will implement the GDPR via The Data Protection Bill 2017 [3], and will include a small number of permitted derogations.

It is apparent that many organisations have turned up late to the game, with up to a third of businesses unaware of GDPR [4] and we see the message further echoed by [5]:

> *"It should really be a 'wake-up call' for every organisation in Europe"*

The current political climate, including the confusion surrounding Brexit have led to some 44% of organisations believing that Brexit will put a stop to GDPR, and a quarter who had started work have cancelled their implementation projects. [6]. Article 83 discusses an "Effective, Proportionate and Dissuasive" penalty structure [1], including the imposition of a 3 month embargo on data processing, €10M and €20M minimum fines it's imperative companies now act.

Most recently (June 2017) the House of Lords concluded that the UK Government and Businesses must act immediately [7]. Meeting the requirements of GDPR will ensure that in the event of the UK withdrawing from the EU, adequacy requirements can be met under Article 45 [1]

II. Objectives

This paper seeks to explore the background and key concepts behind the GDPR, and document the early phases of the implementation project at Runshaw College, utilizing Agile techniques and tools.

Specifically, the project work focuses on three areas:

1. Familiarization with the key concepts and changes surrounding the GDPR.
2. The creation of a Data Protection Impact Assessment (DPIA) [1] template.
3. The implementation of a software system:
   a. to record the key data collected by the DPIA, to form an Information Asset Management system.
   b. to track and facilitate requests regarding data subject's rights under the GDPR.

Due to the nature and volume of changes, future work will be identified and falls beyond the scope of this paper.

III. Background And related work

A. European Convention on Human Rights

The ECHR [8] forms the Overarching legislation, covering matters including that of privacy (and data protection). As a qualified right, the right to privacy can be overridden [9], however additional legislation exists to ensure that any overriding activity must be necessary, proportionate, appropriate and, justified.

B. 1995 EU Data Protection Directive

The first of these pieces of additional legislation arrived with the 1995 Data Protection Directive [10], enacted in the UK as the 1998 Data Protection Act [11].

As a directive (a minimum standard), each member state interpreted and enacted the recommendations in differing ways, with differing levels of protection. This has been seen to prevent the free flow of information between member states, and thus has impacted the economies of Europe [1].

The Directive introduced the eight Data Protection Principles.

Data must be:

1. Fairly & Lawfully processed.
2. Processing for Limited Purposes
3. Adequate, Relevant and not Excessive.
4. Accurate & Up 8to Date
5. Not Kept Longer Than Necessary
6. Processed in Line with Subject Rights.
7. Kept Secure.
8. Not Transferred Overseas Without Adequate Protection.

Figure 1 - The Eight Data Protection Principles [11]

In the 21st Century, the rapid rise of modern technology coupled with the globalization of data flows have left current legislation wanting [12]. We see this most clearly when we look at the vast quantities of data held by social media enterprises [13], often stored in third countries. It is thought that the GDPR will begin to address these issues, specifically where children's data is concerned [14].

Where organizations have subcontracted their data processing activities to third parties who are not as fully regulated, issues have arisen regarding the use and storage of the data. [12][15].

C. General Data Protection Regulation

In recognizing the changing environment, the Council of the European Union in conjunction with the European Parliament authored the General Data Protection Legislation. Recital 7 [1] states:

> *"Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.*
>
> *Natural persons should have control of their own personal data."*

The Regulation is formed of 99 Articles and 173 Recitals. The legislation is referred to as being subjective, and uncertain [16] and this may lead to the ignorance and confusion currently seen [4][6].

.

Chapter	**Title**
i.	General Provision
ii.	Principles
iii.	Rights of the Data Subject
iv.	Requirements on Controllers and Processors
v.	Independent Supervisory Authorities
vi.	Independent Supervisory Authorities
vii.	Cooperation and Consistency
viii.	Remedies, Liability and Penalties
ix.	Provisions Relating to Specific Processing Situations
x.	Delegated Acts and Implementing Acts
xi.	Final Provisions

Figure 2 - GDPR Chapters [1]

Among the key changes, Controllers and Processors are now compelled to meet higher standards, have greater accountability and transparency and meet stricter reporting requirements [17].

The simplified reporting and enforcement processes laid out should result in savings for multinational organizations. They now need only deal with a single Data Protection Authority, the one in the member state where their primary Data Protection function resides.

In Article 5, we see the eight principles of data protection have now been refined and reduced to six:

Principles relating to processing of Personal Data:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimization.
- Accuracy.
- Storage limitation.

- Integrity and confidentiality.
- Accountability.

Figure 3 - GDPR Principles [1]

Article 38 dictates that all but the smallest of organisations must now appoint a named Data Protection Officer, and provides for a clear outline of his/her Role and Responsibilities [18].

Article 33 mandates that where an organization processes Special/Sensitive Data (Defined in Article 9) it must now carry out a Data Protection Impact Assessment. This assessment will explore and document the risks to the rights and freedoms of individuals [19]

Organisations are now responsible for identifying the basis upon which they are collecting and processing information, and this can take a number of forms laid out in Article 6.

- Compliance with a Legal Obligations
- Performance of a Contract
- Protecting a Subject's Vital Interests
- Consent
- Public Interest
- Other Legitimate Interests (unless overridden by the fundamental rights of the data subject)

Figure 4 - Legal Basis for Processing (Article 6) (European Parliament, 2016)

Children, and their ability to consent form the basis of Article 8, and the Regulation stipulates that Parental Consent is required for children under the age of 16. [20]. However, provision is made for individual member states to vary that age, without it becoming lower than 13.

The GDPR permits a number of derogations, of which the most notable to be implemented is that from age 13 a Data Subject will be able to consent to the processing of their data. [3]

Data Controllers have a legal obligation to effect the rights of Data Subjects [1], and a number of new rights are defined:

Article	Right
12	Transparency, Communication and Modalities.
13	Provision of Information regarding the Controller and Processor.
14	Provision of Information regarding data acquired from third parties.
15	Right of Access
16	Right to Rectification
17	Right to Erasure (aka Right to be Forgotten)
18	Right to Restriction of Processing
19	Notification obligations regarding Articles 16-18
20	Right to Data Portability

Figure 5 - Data Subjects Rights (European Parliament, 2016)

Timescales for production of any required information has been reduced to 30 days (with a potential two-month extension) and fees have been abolished.

A number of new financial and non-financial, effective, proportionate and dissuasive penalties can now be levied for non-compliance and where a breach has occurred [1]. The penalties range from a three-month ban on processing to €10M & €20M fines depending on which article has been breached.

Regime	**Higher**	**Lower**
Penalty	4% of turnover or €20M	2% of turnover or €10M
Estimate	£1.4M Approx.	£700K Approx.
Breach Areas:	Lawfulness & Consent Breaches surrounding special categories of data Breaches involving overseas transfer Use of information from a 3rd party Failures to facilitate Subject's Rights Access Erasure Objection Restriction Portability	Data protection by design & default Failure to carry out DPIA Appointment of representatives (DPO) DPO tasks & responsibilities Cooperation with the ICO Security of processing Failures to notify breaches: To ICO To Data Subject

Figure 6 - Penalty Regime [1]

Table 3 highlights the scope of both levels of financial penalty with an estimate of the value for a Further Education College with an annual turnover (Funding Allocation) of £35M.

D. The Data Protection Bill

A Statement of Intent has been issued by Her Majesties Government's Department for Digital, Culture, Media and Sport, to the effect that the UK will implement GDPR via a new Data Protection Bill late in 2017 [3].

Derogations regarding consent, criminal records, automated decision making, research and law enforcement are likely to appear within the legislation [3]

E. Information Asset Management

We can define Information Asset Management as, the philosophy of managing enterprise data, information, and content as an asset in a business and accounting sense [21].

IAM harks back to the concept of Information-Based Organisations [22], that is organisations where Data and Knowledge are used effectively. [23] note that few business are successful in managing Data, Information and Knowledge as assets. In their earlier work, they attribute a number of factors, for example lack of buy in from the Board and Management, not having staff with a wide enough remit to cover the whole organization, and confusion within the IT function [24].

Data mapping exercises can be used to form the basis of IAM, using techniques such as Data Flow Diagrams [25][26]. And more recently refined in the UML 2.0 Standard [27] [28]. These along with inventories of the categories and types of personal information processed and the purposes for which they are stored form the basis of a sound Personal Information Management System [29]

F. Data Protection Impact Assessment

In order to populate an Information Asset Management Database, or Personal Information Management System we can begin by using a technique mandated by the GDPR. That of Data Protection Impact Assessments (DPIA) (Article 35) [1].

The DPIA intends to uncover both the data being processed, and the *"risk to the rights and freedoms of natural persons"* [1]. [19] postulates that the DPIA process mandates a "broad ethical assessment".

A process for the creation of a DPIA has been proposed [30], offering a three stage model.

Phase	**Elements**
A - Preparation	A1 Necessity. A2 Scope. A3 Description & Identification of Data Flows. A4 Identification of Actors & Persons Concerned. A5 Identification of Relevant Legal Requirements. Documentation of Tasks & Issues.
B - Evaluation	B1 Identification of Protection Goals. B2. Identification of Potential Attackers, Motives & Objectives. B3 Identification of Evaluation Criteria and Benchmarks. B4. Evaluation of the Risk.
C - Reporting & Safeguarding	C1. Identification of Appropriate Safeguards. C2. Documentation of Evaluation Results. C3. Report & Publication C4. Implementation of Safeguards. C5. Auditing of Evaluation Results.

Figure 7 - DPIA Process [30]

GDPR Article 35 para. 11 [1] suggests that regular review and revisiting of the DPIA is necessary, and this is echoed by [30]:

> *"A DPIA is not a singular and linear process, but rather has to be repeated to ensure continuous supervision over the lifetime of a project"*

G. Agile Project Management

> *"Agile project management focuses on continuous improvement, scope flexibility, team input, and delivering essential quality products." [31]*

Popularized in the Agile Manifesto [32], Agile Project Management/Agile Software Development is backed by the 12 Agile Principles [32]. These can be regarded as a set of guiding concepts that support project teams [31].

1. Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.

2. Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.

3. Deliver working software frequently, from a couple of weeks to a couple of months, with a preference for the shorter timescale.

4. Business people and developers must work together daily throughout the project.

5. Build projects around motivated individuals. Give them the environment and support they need, then trust them to get the job done.

6. The most efficient and effective method of conveying information to and within the development team is face-to-face conversation.

7. Working software is the primary measure of progress.

8. Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.

9. Continuous attention to technical excellence and good design enhances agility.

10. Simplicity — the art of maximizing the amount of work not done — is essential.

11. The best architectures, requirements, and designs emerge from self-organizing teams.

12. At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

Figure 8 – The 12 Agile Principles [32]

A wide range of Agile Tools, Techniques and Practices exist, each with specific aims and benefits [33]. Teams are able to 'pick and choose' those which they find most effective and fit their needs. It is mostly accepted that Agile Tools and Methods are cost effective and if used carefully can bring about immediate value and productivity improvements [34] [35].

A large number of Agile tools aim to facilitate discussion and collaboration [36], and they become essential in projects with a high degree of uncertainty and change. Themes regarding People and communication resound throughout Agile Research [37], and the work of corporations with a keen interest in Agile Project Management [38].

In a collaborative environment, people are more inclined to share valuable information quickly, [36], collaboration embeds the principle of 'People over Process' [32]. With this in mind, common consequences of failures in collaboration cover issues with requirements capture and prioritization, inability for the team to 'fail early' often due to incomplete feedback [39].

IV. Project

A. *Tools & Techniques*

Throughout the project, a number of Tools and Techniques have been employed. The tools were selected due to their appropriateness and levels of familiarity within the project team. A fully detailed discussion justification of these tools is beyond the scope of this paper.

Analysis, Modelling & Documentation	Rich Pictures [40] UML Use Case Diagram [27] Epics [41] User Stories [41] MoSCoW Priortization [42] Entity Relationship Model [43] Facilitated Workshops [42]
Project Management	Kanban [44] Jira Software [45]
Platform	Jira Service Desk [45]

Table 1 - Summary of Techniques & Tools Utilized.

B. *Stakeholders*

> *"Stakeholders encompass everybody inside or outside the project who are involved in or affected by it." [42]*

Of utmost importance in any software project, is the identification of relevant stakeholders. [46] states that many projects become difficult due to the failure to identify and engage with all of the necessary stakeholders. This view is backed up by the [42] who identify that poor communication is recognized as the major cause of project failure.

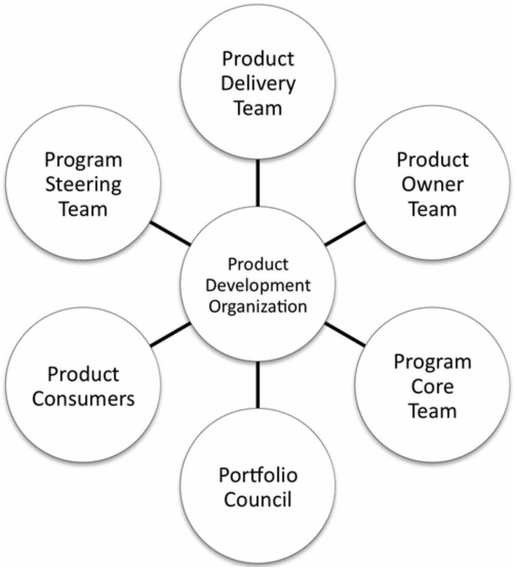

Figure 9 - Primary Stakeholder Groups [46]

Utilizing the model proposed by [46] the following stakeholders have been identified, utilizing four of the six primary stakeholder groups.

Team	Members/Stakeholder(s)
Product Owner	Head of IT Services.
Product Delivery	Head of IT Services. IT Systems Team Leader. Service Desk Team Leader.
Product Sponsor	HR Director. Director of Finance & MIS. Director of Facilities.
Product Consumers	Director of Recruitment, Marketing & Business Development. Head of Quality, Management Information & Student Tracking. QMIST - Data Team. QMIST - Reporting Team. HR Team. Customers: • Staff • Students • Visitors

Table 2 - Project Stakeholders

C. *Foundations*

At the outset of the project a Facilitated Workshop [42] was convened to bring the various stakeholders together. Prior to the workshop the Product Sponsors were consulted and an agenda drafted . This is seen as best practice [42], and allows everyone to start the workshop on an equal footing.

At this workshop the team dedicated time to creating a Rich Picture [40], a visual tool utilised to document a complex scenario.

In line with best practice, the workshop was documented by an appointed scribe. Unfortunately at this stage approval has not been granted for the inclusion of the minutes within this paper.

D. *Aims and Objectives*

During the foundation workshop, The Rich Picture identified a small number of high-priority scenarios, where the implementation of a software system was required.

1. To record the key data collected by the DPIA, to form an Information Asset Management system.
2. To record potential Data Breaches, reporting details and mitigations.
3. To track and facilitate requests regarding data subject’s rights under the GDPR.

These software solutions were prioritised by the Senior Leadership Team for immediate development.

Accompanying the Rich Picture is a Use Case Diagram [27], depicting the relevant Use Cases related to the three objectives.

The three high level objectives, were then re-written in the form of Epics [41] and recorded within the Jira Software [45] system. These epics were prioritized using the MoSCow model [42].

Epic	Priority
As the Senior Data Protection Officer, I want an Information Asset Management Database so that the College's Information Assets can be recorded, managed and have Data Protection Impact Assessments carried out against them.	Should
As the Senior Data Protection Officer, I want a tracking system so that requests regarding Data Subject's rights can be recorded, managed and reported on.	Must
As the Senior Data Protection Officer, I want a tracking system so that Data Protection Breaches can be recorded, managed and reported on.	Must

Table 2 - High Level Epics (Examples)

E. *Project Management*

A Kanban-esque approach has been selected due to the project having just a single developer. The Kanban [44] methodology utilizes visualization techniques, flow management, work in progress limitation and feedback loops to facilitate the creation of software or completion of other task based projects.

Due to the use of Jira Service Desk [45] within the IT Services function, Jira Software [45] was selected as the Project Management tool.

A new project (GDPR) was created, with the Kanban template selected. Epics, User Stories and Tasks can be tracked using this template, and visualized on a Kanban Board.

F. *Architecture*

At a follow up meeting, representatives from the IT Services function concluded that the use of the Jira platform would be preferable to the development of a bespoke software solution.

Jira is used for issue tracking and project management by over 75,000 customers in 122 countries around the globe [45]

Jira is broken down into three sub-products:

Jira Core	Is intended at generic project management and issue tracking.
Jira Software	Agile project management features.

Jira Service Desk	Intended for use by IT or business service desks.

Figure 10 - Jira Product Summary [47]

The core reasoning behind this was that from the onset of the GDPR the Service Desk team will be responsible for the recording of requests related to Data Subject's Rights. The team presently utilize the Jira Service Desk product for Incident, Request and Change Management in line with ITIL [48] best practice.

G. Implementation

A new project was created within Jira, using the Service Desk template. In addition to the features offered by the basic Jira Core template, Service Desk adds complex SLA's, Work Queues, Self Service and Reporting [49].

To allow the creation of custom forms and fields, a Screen Scheme was also created, along with a Field Configuration.

By default, Jira Service Desk generates a large number of e-mail notifications, in order to customize and restrict this, a Notification Scheme was created. It was decided that no communication should emanate from the software solution, in order that the Data Protection team can formulate their own responses taking into account the needs of the Data Subject. To facilitate this the Notification Scheme has all correspondence disabled.

A number of Issue Types have been created within Jira. Issue Types are used to represent data entities and can have fields added by way of Screen Schemes.

Issue Type
Subjects Rights Request
Breach
DPIA
Measure
Risk

Table 3 - Issue Types

1) DPIA & Information Asset Management

A considerable time during the early phase of the project was dedicated to the creation of a standard DPIA form to be used when reviewing or commissioning a project, form or process.

In line with [30] and [50] the group specified a form with supporting guidance, intended to capture the core elements of the DPIA.

In addition, a Microsoft Word template has been authored to allow a more complete document to be created and attached.

Section / Field		**Control Type**
Overview Section		
Summary	Form/Process/Project Name	Text Box / String
Data Subject Classification	Categories of person's data captured. • Staff • Student • Visitor • Governor • Public • Other	Check Box List (Multiple)
Approvers	List of persons required to Approve / Review this DPIA	Jira User Selector / String
Approval Date	Once approved, the date this DPIA was approved	Text Box / Date
Description	High level description of the DPIA.	Text Box / Multi Line String
Background Section		
Legal Basis for Processing Personal Data	Summary of the main aspects covering the legal basis for processing the personal data collected.	Text Box / Multi Line String
Third Party Access to Information	Information surrounding any data which will be shared with third parties.	Text Box / Multi Line String
Screening Questions	In line with the guidance of the ICO, a list of screening questions is presented. If any are answered Yes [Ticked] a DPIA is mandated.	Check Box List (Multiple)
Risks & Security Measures		
Associated Risks	A summary of the potential risks surrounding the collection	Text Box / Multi Line String
Privacy and Related Risks	Pre-defined, risks can be selected from a list. A risk this way can be	Jira Issue Selector (Multiple)

	tracked across multiple DPIA	
Security Measures Overview	A summary of the security measures in place to mitigate the risks.	Text Box / Multi Line String
Security Measures	Pre-defined, security measures can be selected from a list.	Jira Issue Selector (Multiple)

Table - DPIA Record Fields

The DPIA record is facilitated by the way of a Jira Screen , and a Jira Workflow. The Jira Screen Editor allows the fields to be laid out in the three tabs as above.

The Jira Workflow facilitates the movement of the record between its initial creation, review, approval and future archival phases.

Further work in a future phase is required to complete the DPIA and IAMDB. This will complete the Issue Types related to Data Stores and Data Fields along with related fields. A new section will be added to the DPIA screen to track which stores and fields are affected by it.

2) Data Subjects Rights Tracking

The GDPR introduces a number of new rights for Data Subjects and new timescales in which to complete any associated activities. This was prioritized equally with that of Breach Recording and again has been facilitated by way of a Jira Screen and associated Jira Workflow.

Section / Field		**Control Type**
Core Details Section		
Data Subject Classification	A list of possible Data Subject Types • Staff • Student • Visitor • Governor • Public • Other	Check Box List (Multiple)
Subjects Rights Request Type	A list of Subjects Rights • Access • Rectification • Portability • Erasure • Restriction • Objection	Check Box List (Multiple)
Contact Details	• Name • E-Mail Address • Phone Number • Mobile Number	Text Boxes / Single & Multi Line String
Description & Fees		
Description	A description of the request.	Text Box / Multi Line String
Excessive Request	Options to collect fees: • No • Yes – Waived • Yes - Charged	Radio Box List
Excessive Request Fee	The fee to be collected	Text Box / Decimal Value
Assignee	The member of staff handling this request	Jira User Selector / String
Resolution		
Description of Resolution	A description of any data shared. Including any attachments etc.	Text Box / Multi Line String
Date Response Sent	The date the final response was sent to the Data Subject	Text Box / Date

Table 4 - Subjects Rights Fields

Within Jira an SLA has been defined for these Issue Types, in order to meet GDPR's 30-day deadline.

Again the Jira Workflow follows the record through its lifecycle from the request being created, to accepted, to worked upon and resolved. Optional stages allow the extension of the deadline (up to 2 Months) and for the request to be held whilst fees are accepted (if deemed excessive)

3) Breach Tracking

With equal priority given to Breach Tracking, as with Subjects Rights Tracking work has been completed on this section.

As with the DPIA and Subjects Rights, the task has been completed using a Jira Workflow and a Jira Screen.

Section / Field		**Control Type**
Breach Overview		
Data Subject Classification	A list of possible Data Subject Types - Staff - Student - Visitor - Governor - Public - Other	Check Box List (Multiple)
Description	A description of the circumstances surrounding the breach.	Text Box / Multi Line String
Number of Individuals Affected	An estimate of the number of individuals affected by the breach.	Text Box / Integer
Impact	A summary of the potential impact this breach may have.	Text Box / Multi Line String
Consequences	A record of any impact e.g. Financial Loss, Adverse Press etc. as a result of the breach.	Text Box / Multi Line String
Assignee	Identifies the person coordinating the breach.	Jira User Selector / String

Table 5 - Breach Tracking Fields

The Jira Workflow tracks the breach through its initial discovery, reporting to the Information Commissioners Office, communication with Data Subjects, Mitigation and Archival.

4) Jira Queues

In order to manage work within Jira Service Desk, Queues can be created to group items and these are defined by the use of JQL Jira Query Language [45]. The JQL language resembles SQL to a large extent.

Each queue displays the number of requests matching the JQL used to define it, and provides an at-a-glance overview of the work on hand.

Queue	**Description**
Subjects Rights Requests	
All Open	A summary of all open Subjects Rights Requests.
New Requests	New Requests which have been logged and not progressed.
Awaiting Fees	Requests deemed as awaiting fees due to excessive requirements.
Within 30 Day Deadline	Active requests, that are still within the initial 30 day deadline.
30 Day Deadline Breached	Requests which are open, and have exceeded the 30 days allowed.
Within 60 Day Extension	Requests which have been given an additional 60 day deadline
90 Day Extension Breached	Requests which have now breached the extended deadline.
Impact Assessments	
New / Draft	New DPIAs
Awaiting Approval	DPIAs which are awaiting review and approval
Approved / Active	Live DPIAs, these will have the details of who has approved the record.
Archived	A summary of archived DPIA, these can be resurrected, copied and amended if need be.
Breaches	
Reporting Due	Breaches where the 72 hour deadline for reporting is now due.
Open	All open breach records.
Concluded	Breaches which as far as possible have been mitigated, and where required reporting has been completed.

Risks & Measures	
Live	A list of all Live Risks & Measures which can be associated with a DPIA.
Archived	Archived Risks & Measures, these can be resurrected.

Table 6 - Jira Queues

5) *Awareness Raising*

In order to raise awareness of the up-coming GDPR, a short training presentation was devised and delivered at the College's Management Team Conference.

The College's staff numbers exceed 500, and a training presentation and plan will be devised in due course. The GDPR mandates that staff are trained and are aware of their responsibilities, along with the rights of Data Subjects [1].

6) **Limitations**

As previously discussed, as work on the DPIA section was de-prioritized. Presently the project lacks the ability to record details surrounding what categories of Personal Data are

V. Summary and Conclusions

Though previous research has revealed a relatively low up-take of Agile Methods and Techniques within the Further Education Sector [51], an Agile approach to the GDPR Implementation and Software Solution has brought about rapid progress which has met customer requirements.

The early Facilitated Workshop [42] sparked a long and prosperous relationship between all of the project's stakeholders, and Regular Review sessions gave those stakeholders a feeling of ownership. The effects of this type of close collaboration have been noted previously [39].

By utilizing an Agile approach to development, late breaking changes to the prioritization of major features was handled effortlessly and did not result in wasted effort. The Kanban [44] model, allows a fixed number of items to be selected and progressed. This technique ensured that effort was only directed to the items which were of the next highest priority. Had this been a Waterfall [52] managed project, it is likely that a considerable amount of effort will have been expended in analyzing and designing the de-prioritized aspects.

Writing the projects requirements as User Stories [41] resulted in the creation of requirements that could be easily understood by all of the projects stakeholders. Previous research suggests that User Stories are seen as enjoyable and effective [53].

Jira Software has previously been discussed in research surrounding Agile Documentation, and was reported as being widely used and seen as an appropriate and effective tool [54].

As a platform, Jira has facilitated the Rapid development and prototyping required by this project. The documentation utilized has been effective in bringing about the successful development of the projects requirements [49][45].

VI. Further Work

Completion of the final phase of the software solution will take place imminently. Immediately following this, training materials and a training schedule will be devised in order to ensure all Staff have a familiarity with the GDPR.

VII. Future Research

We see from the bleak statistics that a degree of ignorance towards the GDPR exists [6][5]. Little in the way of research exists regarding the implementation of Tools and Processes to support the GDPR within business, and specifically the public and education sectors.

Future work to explore these aspects, as well as a review of breaches and the penalties imposed would become useful tools for Data Protection Practitioners across Europe and beyond.

VIII. Reflection

The use of an external training course and certification in order provide familiarization with the GDPR facilitated a focused approach to the research required to complete the project.

The use Agile methodologies and techniques against a background of the short amount of development time allocated to the project, has resulted in a positive outcome.

A toolbox of Agile techniques such as Rich Pictures [40], UML [28], MoSCoW prioritization [42] has been developed, and will undoubtedly be re-used on future projects.

Acknowledgment

With thanks to colleagues within the College Management Team and IT Services team at Runshaw College.

References

[1] European Parliament, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), vol. 27. 2016.

[2] J. P. Albrecht, "How the GDPR Will Change the World," Eur. Data Prot. L. Rev., vol. 2, p. 287, 2016.

[3] HM Government, Data Protection Bill - Statement of Intent. 2017.

[4] 4D, "Peering into Pandora's Box," vol. 2016, 2016.

[5] P. Rowley, "Navigating Brexit and GDPR," ITNOW, vol. 58, no. 4, pp. 48–49, Dec. 2016.

[6] Crown Records Management, "1 in 4 UK businesses have CANCELLED preparations for GDPR," The Vault: Crown Records Management, 03-Apr-2017. [Online]. Available: https://thevault.crownrms.com/uk-businesses-cancelled-

preparations-gdpr/. [Accessed: 05-Aug-2017].

[7] House of Lords, “Brexit & the EU Data Protection Package.” Autority of the House of Lords, Jun-2017.

[8] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. 1950.

[9] R. Mullender, Tort, human rights, and common law culture. JSTOR, 2003.

[10] European Parliament, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” Official Journal L 281 , 23/11/1995 P. 0031 - 0050;, 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. [Accessed: 05-Aug-2017].

[11] HM Government, “Data Protection Act 1998,” 1998. [Online]. Available: http://www.legislation.gov.uk/ukpga/1998/29/contents. [Accessed: 05-Aug-2017].

[12] V. Reding, “The upcoming data protection reform for the European Union,” International Data Privacy Law, vol. 1, no. 1, pp. 3–5, Feb. 2011.

[13] E. Zheleva and L. Getoor, “To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles,” in Proceedings of the 18th international conference on World wide web, 2009, pp. 531–540.

[14] K. McCullagh, “The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?,” 2016.

[15] D. Flint, “Sharing the Risk: Processors and the GDPR,” Business Law Review, vol. 38, no. 4, pp. 171–172, 2017.

[16] S. Agarwal, “Towards dealing with GDPR uncertainty,” 2016.

[17] S. Davies, “The Data Protection Regulation: A Triumph of Pragmatism over Principle Foreword,” Eur. Data Prot. L. Rev., vol. 2, pp. 290–296, 2016.

[18] P. Lambert, “The Data Protection Officer: Profession, Rules and Role,” 2017.

[19] C. Quelle, “The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing,” 2015.

[20] E. Lievens, “Children and the GDPR: a quest for clarification and the integration of child rights considerations: Panel: Generation Zero-Data & Digital Marketing Protections for Children and Teens under the GDPR, COPPA and the new FCC Privacy Rules,” in Computers, Privacy & Data Protection: The Age of Intelligent Machines, 2017.

[21] J. Ladley, Making enterprise information management (EIM) work for business: A guide to understanding information as an asset. Morgan Kaufmann, 2010.

[22] P. F. Drucker and others, “The coming of the new organization,” 1988.

[23] N. Evans and J. Price, “Information Asset Management Capability: The Role of the CIO,” 2015.

[24] J. Price and N. Evans, “Information Asset Management: Who is Responsible and Accountable?,” in European Conference on Information Management and Evaluation, 2013, p. 129.

[25] E. Yourdon and L. Constantine, Structured Design: Fundamentals of a Discipline of Computer Program and Systems Design, copyright 1979 by Prentice-Hall. Yourdon Press, 1979.

[26] C. P. Gane and T. Sarson, Structured systems analysis: tools and techniques. Prentice Hall Professional Technical Reference, 1979.

[27] Object Management Group, “UML 2.0 Superstructure Specification,” OMG, Needham, 2004.

[28] S. W. Ambler, The object primer: Agile model-driven development with UML 2.0. Cambridge University Press, 2004.

[29] B. S. BSi, “10012: 2009–Data protection,” Specification for a personal information management system, 2009.

[30] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, “A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation,” in Annual Privacy Forum, 2016, pp. 21–37.

[31] M. C. Layton, Agile project management for dummies. John Wiley & Sons, 2012.

[32] K. Beck et al., “Manifesto for agile software development,” 2001.

[33] A. Cockburn, “What the Agile Toolbox Contains,” CrossTalk, 2004.

[34] D. Parsons, H. Ryu, and R. Lal, “The impact of methods and techniques on outcomes from agile software development projects,” Organizational Dynamics of Technology-Based Innovation: Diversifying the Research Agenda, pp. 235–249, 2007.

[35] I. Vacari and R. Prikladnicki, “Adopting Agile Methods in the Public Sector: A Systematic Literature Review,” presented at the SEKE, 2015, pp. 709–714.

[36] A. Cockburn and J. Highsmith, “Agile software development, the people factor,” Computer, vol. 34, no. 11, pp. 131–133, 2001.

[37] P. Gregory, L. Barroca, H. Sharp, A. Deshpande, and K. Taylor, “The challenges that challenge: Engaging with agile practitioners’ concerns,” Information and Software Technology, vol. 77, pp. 92–104, 2016.

[38] Agile Business Consortium, “The 9 Principles of Agile Leadership.” 2017.

[39] R. Hoda, J. Noble, and S. Marshall, “The impact of inadequate customer collaboration on self-organizing Agile teams,” Information and Software Technology, vol. 53, no. 5, pp. 521–534, 2011.

[40] P. Checkland and J. Scholes, “Soft systems methodology in action,” New York (US): John Wiley & Sons, 1990.

[41] M. Cohn, User stories applied: For agile software development. Addison-Wesley Professional, 2004.

[42] Agile Business Consortium, “The DSDM Agile Project Framework (2014 Onwards),” Agile Business Consortium, 09-Nov-2015. [Online]. Available: https://www.agilebusiness.org/content/people-teams-and-interactions. [Accessed: 06-Aug-2017].

[43] P. P.-S. Chen, “The entity-relationship model—toward a unified view of data,” ACM Transactions on Database Systems (TODS), vol. 1, no. 1, pp. 9–36, 1976.

[44] D. J. Anderson, Kanban: successful evolutionary change for your technology business. Blue Hole Press, 2010.

[45] Atlassian, “Atlassian | Software Development and Collaboration Tools,” Atlassian, 2017. [Online]. Available: https://www.atlassian.com. [Accessed: 06-Aug-2017].

[46] K. Power, “Stakeholder Identification in Agile Software Product Development Organizations: A Model for Understanding Who and What Really Counts,” in 2010 Agile Conference, 2010, pp. 87–94.

[47] Wikipedia, “Jira (software),” Wikipedia. 06-Aug-2017.

[48] The Stationary Office, ITIL. TSO, 2008.

[49] P. Li, Jira 7 Essentials. Packt Publishing Ltd, 2016.

[50] Information Commissioners Office, Conducting privacy impact assessments code of practice. 2014.

[51] A. Harding and J. C. Read, “A Study into the Adoption of, and Enthusiasm for Agile Development Methodologies Within Further Education.,” 26th International Conference On Information Systems Development (ISD2017 Cyprus), 2017.

[52] W. Royce, “The software lifecycle model (Waterfall Model),” in Proc. WESTCON, 1970.

[53] G. Lucassen, F. Dalpiaz, J. M. E. M. van der Werf, and S. Brinkkemper, “The Use and Effectiveness of User Stories in Practice,” in Requirements Engineering: Foundation for Software Quality, 2016, pp. 205–222.

[54] C. J. Stettina and W. Heijstek, “Necessary and neglected?: an empirical study of internal documentation in agile software development teams,” in Proceedings of the 29th ACM international conference on Design of communication, 2011, pp. 159–166.