Essex County Council

# Project Initiation Document

# Implementation of the General Data Protection Regulation within ECC

# Document Control

## Document Information

| | Information |
|---|---|
| Document Owner | Scott Sammons |
| Issue Date | 27.02.2017 |
| Last Saved Date | 27.02.2017 |
| File Name | *20170227- GDPR Implementation Project PID* |

## Document History

| Version | Issue Date | Changes |
|---|---|---|
| 0.1 | 27/02/2017 | First Draft |
| 0.2 | 11/03/2017 | Revised Draft |
| 0.3 | 20/03/2017 | Revised Draft |
| 0.4 | 27/03/2017 | Initial Final Draft ready for Board Review |
| 1.0 | 29/03/2017 | Approved at Project Board |

## Document Approvals

| Role | Name | Approved | Date |
|---|---|---|---|
| Project Sponsor | Margaret Lee | | 29/03/2017 |
| Project Manager | Scott Sammons | | 29/03/2017 |
| Project Board | Various | | 29/03/2017 |
| Project Working Group | Various | | 27/03/2017 |
| Information Governance Representative | Lauri Almond | | 29/032017 |
| Data Protection Officer | Gill Furlong | | 29/03/2017 |

## Document Distribution

| Name | Role | Date of Issue | Version |
|---|---|---|---|
| Members of the Project Board | | 27/03/2017 | 0.4 |
| Members of the Project Team | | 24/03/2017 | 0.4 |

# Table of Contents

# 1 Project Summary

There is a legal requirement for ECC as a Public Authority to address compliance with the incoming General Data Protection Regulation (GDPR) by 25 May 2018. Although the UK has voted to leave the EU and the government has committed to enacting Article 50 by March 2017, the Government has also outlined that the UK will keep all EU legislation in order to continue conducting business with the EU, until such a time as the Government can create suitable replacement UK legislation. Therefore the GDPR and its UK specific derogations will apply to ECC and ECC will need to implement the requirements of them accordingly.

The key purpose of this project is to assess the new legislation and the impact on ECC, determine what gaps there are in current and future required controls and seek to implement those controls based on their level of risk. It is accepted that the Council will not be able to achieve 100% compliance by May 2018 as the Regulation is too large and the Authority's processing too complex. However key controls can be implemented to give ECC a strong framework for managing compliance into and post May 2018.

# 2 Project Definition

## Project Objectives

1. Create a framework and environment for ECC to become GDPR compliant by 25 May 2018
2. Build GDPR compliance into policies and procedures at ECC to enable ECC to become compliant and continually assess its compliance with the GDPR
3. Increase training and awareness to staff on data protection, in line with the GDPR
4. Create Data Protection Officer (DPO) job description and role
5. Implement all high risk areas of change within ECC be that to technology, systems or processes.

## Project Deliverables

| Ref | Deliverable | Comments |
|---|---|---|
| DEL-1.1 | Revised policies and procedures | Changes to all policies and procedures to accommodate GDPR requirements. This includes determining changes, applying changes and approving changes through normal governance processes. |
| DEL-1.2 | Revised Privacy Impact Assessment Process | Changes to PIA process and templates to accommodate GDPR requirements. This includes determining changes, applying changes and approving changes through normal governance processes. |
| DEL-1.3 | Agreed risk approach & framework | Determine and agree risk management approach for project and wider framework. |
| DEL-1.4 | Implementation of the GDPR Data Protection Officer Role | Scope requirements, gap analysis, options paper for approval then implementation of the GDPR DPO role. |
| DEL-2.1 | Revised Internal Assurance Programme | Scope requirements, gap analysis, then implementation of any internal assurance requirements. |
| DEL-2.2 | Revised External Assurance Programme | Scope requirements, gap analysis, then implementation of any external assurance requirements. |
| DEL-3.1 | List of Third Parties processing Personal Data | Create a list of third parties processing personal data with risk rating if possible. |

| | | |
|---|---|---|
| DEL-3.2 | Develop standard set of DP contract terms for use | Create standard terms for contracts and data sharing agreements, aligned with WESIF, for use within IG and Commerical. |
| DEL-3.3 | Agree approach and implementation plan for high risk 3rd parties. | Based on list of third parties, agree prioritisation approach and workplan. |
| DEL-4.1 | Update revised privacy notices and process to maintain them | Scope requirements, gap analysis, then implementation of any changes needed to privacy notices. This includes agreement on a process to maintain them. |
| DEL-4.2 | Update website privacy notice & policy, including process to maintain it | Scope requirements, gap analysis, then implementation of any changes needed to website privacy policy. This includes agreement on a process to maintain them. |
| DEL-4.3 | Scope, build and implement methods for managing consent | Scope requirements, gap analysis, then implementation of any changes needed to enable management of consent based processing. This includes agreement on a process to maintain them. |
| DEL-4.4 | Complete development and implementation of Record of Processing Activites database | Finish current development of the ROPA database and produce analysis of it's findings. |
| DEL-5.1 | Agree and publish retention periods based on condition for processing | Review current retention regime, determine any gaps, and based on the ROPA findings identify where any issues may need addressing. |
| DEL-5.2 | Establish and implement process for managing and monitoring retention periods | Review current process to incorporate GDPR requirements |

| | | |
|---|---|---|
| | | and approval through the normal methods. |
| DEL-5.3 | Agree and establish a process for the destruction of personal data when no longer required. | Review current process to incorporate GDPR requirements and approval through the normal methods. |
| DEL-6.1 | Implement changes to IG related complaints process | Scope requirements, gap analysis, then implementation of any changes needed to complaints process. This includes agreement on a process to maintain and report on them. |
| DEL-6.2 | Agreed revised process for handling requests regarding personal data | Scope requirements, gap analysis, then implementation of any changes needed to SAR process. This includes agreement on a process to maintain and report on them |
| DEL-6.3 | Agreed revised guidance and resources for FOI & SAR handling | Determine changes to FOI/EIR and SAR handling and draft guidance docs for team. |
| DEL-6.4 | Scope and agree requirements for Data Portablity requests | Determine services in scope and review processes to determine what changes are need for Data Portability. Where changes are needed agree and implement these accordingly. |
| DEL-7.1 | Agree and implement incident response process | Scope current process, determine gaps with GDPR, agree and implement changes to fill the gaps. |
| DEL-7.2 | Scope and implement encyption standards | Scope current process, determine gaps with GDPR, agree and implement changes to fill the gaps. |

| | | |
|---|---|---|
| DEL-7.3 | Document current security controls and identify any gaps | Scope current controls, determine gaps with GDPR, agree and implement changes to fill the gaps. |
| DEL-7.4 | Document current data integrity controls and identify any gaps | Scope current controls, determine gaps with GDPR, agree and implement changes to fill the gaps. |
| DEL-7.5 | Document current business continuty controls and identify any gaps | Scope current controls, determine gaps with GDPR, agree and implement changes to fill the gaps. |
| DEL-8.1 | Collate and scope required system changes | Collate all system changes into a 'shopping list'. Rank them based on risk and resource needed. Agree and develop implementation plan for up to and post May 2018. |
| DEL-8.2 | Collate and scope required data portablity system changes | Based on above work, collate system changes needed and agree implementation plan. |
| DEL-8.3 | Collate and scope anonymisation standards and implement process to sustain | Collate and scope anonymisation standards within analytics / IT and implement process to sustain |
| DEL-9.1 | Scope and deliver training programme for key roles (DPO, IG Team etc) | Determine key roles, determine gaps in knowledge, agree and deliver training programme. |
| DEL-9.2 | Scope and deliver ongoing project team awareness programme | Ongoing key messages and updates for stakeholders and key roles. |
| DEL-9.3 | Scope and deliver all ECC awareness change management programme | Based on work above and below, where changes will affect staff ensure these are managed in accordance with ECC change management expectations. |

| | | | |
|---|---|---|---|
| | DEL-9.4 | Scope and deliver ongoing all staff awareness and training programme | Scope changes needed to current e-learning package. Deliver changes and re-launch DP training package for all staff. |
| | DEL-10.1 | Define & deliver changes to staff employment contracts & policies | Define & deliver changes to staff employment contracts & policies dependant on UK law changes (currently not specified). |
| | DEL-10.2 | Define & deliver changes to staff rights management processes | Define & deliver changes to staff employment rights dependant on UK law changes (currently not specified). |

## Project Approach

Work streams will be sequentially undertaken to implement the GDPR compliance framework and controls for ECC. Each Workstream will have a leader and team to help delivery of the required controls.

Most of the tasks will be implemented by internal activities and staff. It is not foreseen at project initiative for the need for external spend.

As many ECC systems hold personal data, input from relevant system owners and developers may be required to prepare recommendations for such systems to become compliant with GDPR.

The order in which these are proposed is as followed:

| Work streams | Due Dates |
|---|---|
| **1. Governance**<br>• Delivery of DPO, policies and procedures, risk framework etc. | March 2018 |
| **2. Assurance**<br>• Delivery of internal and external assurance requirements | May 2018 |
| **3. Third Party Management**<br>• Delivery of ongoing contract management and data sharing frameworks | May 2018 |
| **4. Data Collection & Use**<br>• Delivery of changes to how and where we collect data from data subjects inc. changes to privacy notices, website policies and | December 2017 |

| | |
|---|---|
| the Register of Processing Activities. | |
| **5. Retention & Disposal**<br>• Defined retention periods, process for destruction and process for advising data subjects of retention periods. | December 2017 |
| **6. Rights**<br>• Delivery of processes and policies for managing data subject's rights | December 2017 |
| **7. Security**<br>• Delivery of required security controls including incident response, encryption and integrity & avaliablty controls | March 2018 |
| **8. Systems and Technology**<br>• Delivery of any required systems or technology changes needed to comply with GDPR controls. | May 2018 |
| **9. Training & Awareness**<br>• Delivery of a training and awareness programme during the project and post project. | May 2018 |
| **10. Staff Data**<br>• Delivery of all required changes needed to process staff data for employment purposes | December 2017 |

## Project Scope

In scope:

- Any and all ECC policies, procedures and controls that have any impact on GDPR and the Police & Crime Data Directive Compliance.
- Any and all ECC service areas that process Personal Data.
- Any and all ECC systems and technology that enables the processing of Personal Data.
- Any and all third parties that process Personal Data on ECC's behalf or jointly.

- Delivery of required controls expressly detailed in the GDPR.
- Delivery of an implementation plan for controls that cannot be delivered by May 2018, which are not expressly detailed in the GDPR, based on an agreed risk approach.
- Maintaining awareness of the project and changes both within the project team and the wider ECC staff base.

Out of Scope:

- Ensuring 100% compliance with GDPR is out of scope for this project as some of the IT system issues may be too complex to resolve within this projects timeline.
- Delivery of awareness or training for third party members of staff or members of the public.
- Delivery of any changes to controls that are owned or managed by third parties.
- Development of commercial products on GDPR for ECC use.
- Involvement with projects and suppliers that do not use personal data

## Constraints

Constraints that need to be considered are:

- Potential changes to GDPR before it comes into effect 25 May 2018 may change scope, quality and time of project
- Potential constraint on resources required – reliant on availability of members of staff currently balancing other pressures and initiatives
- Framework for compliance must be completed in time to allow ECC to become compliant with GDPR by 25 May 2018

## Assumptions

- GDPR requirements will not change fundamentally between now and May 2018
- It is assumed that the UK Government process for recinding the UK DPA and creating appropriate UK derogations is completed in a timely manner.
- It is assumed that adequate internal staff time will be available to run this project according to timescales
- It is assumed that existing policies and procedures can be easily reviewed and updated
- It is assumed that ECC has already documented legal retention periods for personal data under UK law
- It is assumed that ECC DLM and ROPA intiatives have delivered the

required information on processing activities

- It is assumed that the current Learning & Development application system will be suitable for this project
- It is assumed that this project will have access to IG staff and has been budgeted for in this project.
- It is assumed that ECC commercial resource will be in place to address ongoing updates to third party contracts on a rolling basis

## 3 Initial Business Case

The project is being driven by legislative regulation to be compliant with the incoming General Data Protection Regulation (GDPR) 2016, which will be replacing the Data Protection Act 1998, and the police and crime directive 2016 (PCD). The GDPR is the Regulation that is set to ensure businesses and organisations collect, process and delete personal data in a fair and secure manner to protect data subjects. The project will carry out an assessment of the GDPR's effect on ECC by providing a GDPR framework that ECC will use to become GDPR & PCD Compliant.

In order to demonstrate compliance, ECC must undertake measures to:

1. Implement appropriate technical and organisational measures that ensure and demonstrate compliance with the GDPR, such as policies, staff training, internal audits of processing activities and reviews of internal HR policies
2. Maintain relevant documentation on processing activities
3. Where appropriate, appoint a Data Protection Officer
4. Implement measures that meet principles of data protection by design and data protection by default
5. Use data protection impact assessments where appropriate
6. Report breaches of the GDPR in a timely manner
7. Be aware and effectively manage GDPR risks
8. And any other legal requirement as yet undefined by these legislation.

Benefits:

1) Reduced risk of incurring large fines for non-compliance and breaches to personal data
2) Increased training and staff awareness on GDPR compliance
3) Updated policies and procedures in line with GDPR
4) Data Protection as a business benefit not a compliance hindrance
5) Increasing residents trust in ECC to handle it's personal data in a fair and transparent manner

## Why this project should go ahead

The replacement of the DPA 1998 with the GDPR is the primary reason to undertake this project, as ECC collects and processes personal data of its residents and staff for various business functions. All organisations that handle personal data will be required to have a reasonable level of compliance prior to 25 May 2018, especially public authorities who are expressly called out in the GDPR.

Another key driver the PCD, around which there is some uncertainty and will require some UK domestic legislation to fully cover the processing of this special category of personal data.

On a related note, over the last 3-4 years ECC has built up a strong relationship with the ICO and has put several measures in place which are now seen as industry leading. In order to protect and enhance this status, which will assist with various strategic information initiatives, ECC should implement GDPR requirements sooner rather than later. Where possible, documenting its operational knowledge in this area to share with partners where appropriate to support Partnership working.

## 4 Benefits and Tracking

| Ref | Project Benefit | Who does this benefit? | When will it be realised? | How will it be measured? |
|---|---|---|---|---|
| B-01 | Faster identification and resolution of personal data breaches by providing training and communicating clear and sustainable procedures for reporting breaches. | All ECC | Following the Project | Presently takes 6 weeks to identify a personal data breach. This timing should be reduced following the project. |
| B-02 | Increased awareness amongst staff on how to handle Personal Data correctly and effectively | All ECC | Following the Project | The time it takes to report a personal data breach will be reduced. Pass rates of previous training on data protection will also be reviewed to measure this benefit |

| | | | | |
|---|---|---|---|---|
| B-03 | A refreshed and up to date compliance framework and structure for 2018 & beyond. | All ECC | Following the Project | Delivery of changes as part of project based on clearly defined scope |

## 5 Budget Approach & Recording

There is currently no central assigned budget for the project and its deliverables. There is some budget availability within the Digital Foundations Programme and this will be explored as the DFP starts to take shape. There is also, at this stage, no easy way of determining the exact amount of funds needed to implement some of the critical requirements of the GDPR.

It is therefore proposed that staff time and resourcing requirements will be recorded as part of the project projections and monitoring. Costs external to ECC, for example in any third party system development, will be raised as and when the project discovers them and will be put to the project board for review.

Budget & cost issues will be reported bi-weekly through the project team and bi-monthly through the project board. Any urgent budget issues will be submitted to the project board electronically for discussion.

## 6 Timescales

**Key milestones for project:**

| | |
|---|---|
| **Feb 2017** | 1. Initial Awareness Campaign Launched |
| **Mar 2017** | 1. Completion of Data Inventory & GAP analysis<br>2. Risk Management Approach Agreed |
| **April 2017** | 1. Standard Contract Terms Agreed<br>2. List of high priority contracts / DS agreements<br>3. Revised complaints process<br>4. Key role training programme agreed |
| **May 2017** | 1. Data Portability Requirements defined<br>2. Agreed Anonymisation standards |
| **June 2017** | 1. Agreed Data Portability Process |
| **July 2017** | 1. Revised PIA process implemented<br>2. Internal Assurance Regime agreed<br>3. Website privacy policy changes agreed |

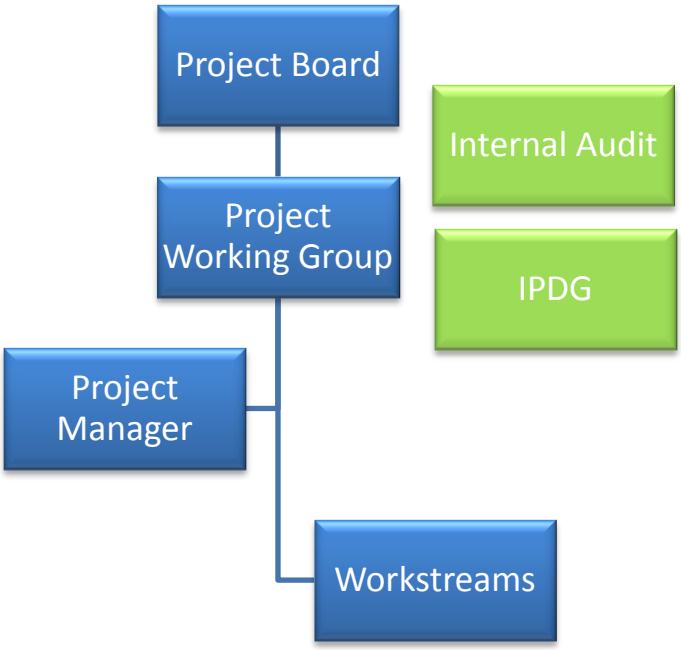
| | |
|---|---|
| | 4. Retention periods & policy agreed<br>5. Incident response process agreed |
| **October 2017** | 1. External Assurance Regime agreed<br>2. Notice & Consent management agreed<br>3. All employee training programme agreed |
| **December 2017** | 1. Changes to website complete<br>2. Revised policies and procedures in place<br>3. Encryption standards in place<br>4. Security & Integrity Controls documented<br>5. Employee data changes made<br>6. DPO role agreed & implemented |
| **January 2018** | 1. All staff training programme deployed<br>2. Key staff training programme deployed |
| **February 2018** | 1. SAR & FOI process & resources deployed<br>2. Data Portability process deployed |
| **March 2018** | 1. Governance Framework fully deployed<br>2. Assurance programme deployed<br>3. Retention and Destruction programme deployed |
| **May 2018** | 1. Accepted level of third parties on new terms<br>2. All high risk system changes now in place<br>3. Completion of project awareness campaign<br>4. Go-Live of GDPR legislation in the UK |
| **June 2018** | 1. Closure of Project. |

## Risks and Controls

| ID | Risk | Control(s) |
|---|---|---|
| R-01 | Project cannot meet the required deadline of the 28th May 2017 | 1) Agree risk management approach. Prioritise resources. Monitor enforcement approach by ICO |
| R-02 | ECC Systems may not be able to be upgraded before May 2018 resulting in increased risk of regulatory action/complaints from data subjects | 1) Feed GDPR requirements into other current, relevant projects as quickly as possible |

| | | |
|---|---|---|
| | | 2) Identify changes required as quickly as possible and deliver changes and recommendations to business as quickly as possible |
| R-03 | Internal knowledge and resources become unavailable resulting in a delay to the project or the need to rely on external resources therefore increasing project costs | 1) Agree prioritisation of resourcing with other projects |
| R-04 | There is not suitable time to implement required system and technology changed as there is no suitable IT resource available | 1) Confirm changes as soon as possible. Prioritse high risk areas first so resourcing can be scoped. |

## 7 Project Organisation Structure




| Role | Name | Responsibility |
|---|---|---|
| **Project Sponsor** | Margaret Lee | Ultimately responsible for the project. Ensures the project is focused throughout its life on achieving its objectives and delivering deliverables that will achieve the forecast benefits. |
| **Senior User(s)** | IPDG | Responsible for approving the deliverables that form part of the |

| | | |
|---|---|---|
| | | ongoing compliance framework. |
| **Senior Suppliers(s)** | Lauri Almond, IG Operations Lead | Represents the interests of those designing, developing, facilitating, procuring and implementing the projects products. This role is accountable for the quality and integrity of the products being delivered. |
| **Project Manager** | Scott Sammons, IG Strategy Lead | Responsible for ensuring the project produces the required products within specified tolerances of time, cost, scope, quality, risk and benefits. The PM has the authority to run the project on a day-to-day basis on behalf of the Project Board, within specified constraints. |
| **Project Board Members** | Margaret Lee (Sponsor)<br>Digital Director<br>Commerical Director<br>Head of Internal Audit<br>Monitoring Officer<br>Head of Information Governance<br>Head of Legal Services<br>Head of Coporate Services<br>Caldicott Guardian | The Project Board is responsible for overseeing the project supporting the sponsor to ensure the project delivers on time, meets stakeholder needs and expectations and delivers its benefits. |
| **Project Team Members** | Project Manager<br>IG Ops Lead<br>Head of IG<br>Records Manager<br>Audit Representative<br>HR Representative<br>Comms Representative<br>Legal Representative<br>IT Security Representative<br>Business Support Representative<br>Adults Social Care Representative<br>Childrens Social Care Representative<br>Commerical Representative<br>Payroll Representative<br>Customer Service Representative | The Project Team are responsible for delivering the detailed actions needed to implement the project deliverables. |

## 8 Communication Plan

| Stakeholder | Nature of Communication (what and how) | When |
|---|---|---|
| Project Board | Meetings/Emails | Bi-Monthly |
| Project Team | E-mails/Meetings | Bi-Weekly |
| Stakeholders | E-mails/Workshops | At key milestones |
| ECC Staff | E-mails/Face to Face events/Intranet Articles | At key milestones |

## 9 Project Quality Plan

The Project Board will be required to review all major project outputs and sign off where possible. This includes key products such as;

- Data Inventory
- Recommendations for updating ECC Systems with GDPR Regulations
- Training programme
- Resources and position of the Data Protection Officer
- Governance Framework (specific policies will be approved by their operational committees).
- Assurance Framework

Key deliverables will be reviewed by SME's and key stakeholders via the project team meetings. Every deliverable will have oversight from the Head of IG, the DPO role once in place and the IG Operations Lead.

All deliverables will have appropriate documentation ready for handover to business as usual responsible staff. Each handover will be fully documented with written acceptance that the product is now accepted by the operational function.

Internal audit are included in the project team and are on the project board (different representatives). Reporting on progress, issues, risks and budget will be completed bi-weekly for the project team and bi-monthly for the project board.

## 10 Project Monitoring

- Project team will provide regular updates to key stakeholders via employee comms and specific awareness events.
- All staff will be updated via key channels at key points during the project lifecycle.
- Recommendations for changing ECC Systems will be written with SMEs

- Project highlight reports will be submitted to the project team bi-weekly.
- Project highlight reports will be submitted to the project board bi-monthly.

| Control Mechanism | Description (including when/ freq) | Owner |
|---|---|---|
| Core Team Scrums | Weekly | Project Manager |
| Highlight Reports | Bi-Weekly | Project Manager |
| Project Boards | Bi-Monthly | Project Sponsor |
| Workstream Team Meetings | Weekly or Monthly, dependent on size of work stream | Project Manager |
| Exception Process | Escalate to Project Board | Project Manager/Project Board |

## 11 Initial Project Plan

## Resource Requirements

**Internal Resources to be available:**

- **IT Resources**
  - IT Security
  - System Development
- **Service Area Representatives**
  - Adults
  - Childrens
  - Commercial
  - Customer Services
  - Internal Audit
  - HR
  - Legal
  - Payroll
  - Employee Comms
- **Information Governance**
  - IG Business Consultant (Ops)
  - IG Business Consultant (Strategy)
  - IG Officers x3

**External Resource:**

- None currently identified

## Tolerances

- There is a 1 month time tolerance on updating policies and procedures to ensure enough time is provided for review and sign-off from management

# 12 Change Control

Change requests and their supporting business case (including GDPR legal changes) to the project will be recorded by the project manager in the Change Log. These will then be evaluated by the project board for approval for inclusion in the project.

Changes to any ECC systems to become GDPR compliant will be submitted via the normal systems change controls process.

Changes to policies and procedures will be approved by their respective approvals processes. In most cases this will be through the IPDG.