

group policies and procedures

# Data Protection by design and default

|  |  |
| --- | --- |
| Category | Corporate Governance |
| Author | Castleman Healthcare Ltd |
| Responsible Director | Dominic Hennessy |
| Date of issue | Dec 2018 |
| Next review date | Dec 2019 |
| Document ref & version | JL v1. |

**Related policies and guidance**



**Document revision and approval history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Approved by | Comments |
| V1 | Dec 2018 | JL | Castleman Healthcare Ltd. |  |
|  |  |  |  |  |

# Data protection by design and default

## **At a glance**

* The GDPR requires all companies processing data to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is ‘data protection by design and by default’.
* In essence, this means Castleman Healthcare Ltd integrates data protection into all our processing activities and business practices, from the design stage right through the lifecycle.
* This concept is not new. Previously known as ‘privacy by design’, it has have always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.
* Data protection by design is about considering data protection and privacy issues upfront in everything the Company does. It can help us ensure that we comply with the GDPR’s fundamental principles and requirements, and forms part of the focus on accountability.

## **Checklists**

☐ Castleman considers data protection issues as part of the design and implementation of systems, services, products and business practices.

☐ Castleman makes data protection an essential component of the core functionality of our processing systems and services.

☐ Castleman anticipates risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

☐ Castleman only processes the personal data that we need for our purposes(s), and that we only use the data for those purposes.

☐ Castleman ensures that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

☐ Castleman provides the identity and contact information of those responsible for data protection both within our organisation and to individuals.

☐ Castleman adopts a ‘plain language’ policy for any public documents so that individuals easily understand what we are doing with their personal data.

☐ Castleman provides individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ Castleman offers strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ Castleman only uses data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When Castleman uses other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ Castleman use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

# Introduction

This policy determines how Castleman Healthcare Ltd. will foster a culture of privacy by design in the way it conducts its business. Whenever a piece of work starts which involves using information about a person’s personal data the risks associated with each project will be assessed.

Castleman will ensure data protection principles are met. This is called a Data Protection Compliance Check. For matters that, if not properly addressed, might involve a risk to privacy, the Data Protection Officer will carry out a Data Protection Impact Assessment.

Projects may be delayed or halted if data protection matters are not fully risk assessed and sign-off obtained from the relevant parties.

# when to perform a risk assessment

Risk assessments should start early so that results can be built into the wider project plan. Risk assessment and risk mitigation will evolve throughout the project until its final completion.

A SMART (**Specific, Measurable, Attainable, Relevant and Timely**) must be assessed performed and assessed.

# date protection risk assessment

In discussion with the project instigator, a rating of high, medium or low data protection risk will be allocated following the SMART assessment. This will determine the level of data protection assurance that will be required.

Identified risks will be transferred to a the project plan and RAG rated, the actions of which shall be worked through methodically until all areas are rated as GREEN.

It is important that this is completed as early as possible in projects as some data protection requirements (such as the location of data storage or the capability to delete data) are non-negotiable in law and can mean that a project has to be abandoned or amended, regardless of the work which has gone on up to that point.

The Information Asset Register will be updated by the Data Protection Officer to reflect the new or amended use of personal data that the project has instigated.

# Data compliance check – low and medium risk

Low or medium risk projects should still follow the Data Protection Compliance Check process which consists of a checklist of matters the project manager will need to address in order to safeguard and manage the personal data that will be collected.

The Compliance Check provides assurances that data has sufficient safeguards and is being collected, used and stored in accordance with data protection principles. Its complexity will vary depending on the data and systems involved. This will ensure all relevant data protection risks and requirements have been considered.

Once completed, the Data Protection Compliance Check will be signed off by the Data Protection Officer and saved in the GDPR section of the Castleman Drop Box.

The proposal may not become operational until identified data protection and RAG ratings have been completed.

# Data compliance check – high risk processing

High risk projects will have a Data Protection Impact Assessment performs. This ensures an in-depth analysis at the application of data protection and cyber security requirements, the associated risks and how they may be mitigated. Any high risk processing must have sufficient safeguards applied to minimise any risk.

Failure to do so could result in the Data Protection Officer or the Information Commissioner’s Office vetoing the processing.

High risk processing is likely to be where there is a significant change in the way in which personal information is used. This is likely to be where:

 The project or proposal has a wide scope

 It uses new or intrusive technologies

 Particularly sensitive or high risk data or individuals are involved

 Information was collected for one purpose but is now intended to be used for another.

 Implementing a new or unusual type of technology

 Implementing new monitoring, surveillance or testing procedures

 Using special category (sensitive) personal data, or the scope of personal data increases

 Consolidating information held by separate parts of our organisation

 Using personal data already held for a new purpose

 Taking action in relation to a new grouping or demographic of identified individuals

 Sharing personal data, or pooling or linking data with additional organisations

Successful completion of the Data Protection Impact Assessment will involve a team with a range of expertise and skills who have an understanding of the project’s aims and the organisation’s culture. This team will have authority to influence the design and development of the project and participate in decisions and will have expertise in privacy and compliance matters, expertise in technology, processes and activities relevant to the project. The team will assess and communicate organisational risks, assess which privacy solutions are feasible for the relevant project and communicate effectively with stakeholders and management.

Data protection legislation requires the advice of the Data Protection Officer to be sought when carrying out a DPIA and depending on the nature of the data processing and the aims and ambitions of the project the team will work with the project manager to identify how the DPIA process will be managed. This will then need to be built into the project’s plans.

Once data protection and strategic fit risks have been managed to the satisfaction of the Data Protection Officer, the final sign-off will come from the Castleman Board.

As Data Protection Impact Assessments are reserved for high risk proposals, it is essential that sufficient time is allowed for proper consideration to take place.

The project may not become operational until any identified data protection issues have been resolved.

# data protection risk assessment

|  |
| --- |
| **Project Manager:** |
|  |
| **Name of proposed project:** |
| **What is the anticipated project start date?** |
| **Describe the project:** |
| **Which of the following types of personal data will you process?** |

**What number of people’s personal data do you expect to process?**

|  |  |
| --- | --- |
| **1-50** |  |
| **51-500** |  |
| **501-1000** |  |
| **1001-10,000** |  |
| **10,000-100,000** |  |
| **100,000 plus** |  |

**Will you be sharing the data with anyone? If so, who?**

**Will you be sending the data off site (this may be electronically or physically)**

**Will you be asking a third party to process data on your behalf? If so, please explain**

**What type of technology or equipment will you be using (if any)?**

**e.g. App/website/software/systems/hand held device**

**Will you be using personal data you already have, but for a new purpose?**

**Will you be undertaking monitoring or surveillance of people as part of this proposal?**

**Does your proposal relate to vulnerable or high risk individuals?**

**Will you be processing the data of children?**

**Date form completed**

**Completed by**

**When completed, send this form to** [**james.leyland@dorset.nhs.uk**](mailto:james.leyland@dorset.nhs.uk)

|  |
| --- |
| **For Data Protection Officer Use:** |
| **Assessed Data Protection Risk (High/Medium/Low)** |
| **Assessed by** |
| **Date** |