# Data Protection Impact Assessment

**Product**: CATCH
**Date:** 28th March 2019

## Step 1: Identify the need for a DPIA

| |
|---|
| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| CATCH is a free health app for parents and carers of children aged 0-5. The app empowers users with the information necessary to decide when they need medical treatment or when self-care is more appropriate.<br>The CATCH app does collect Usage Data and does request Personal Data.<br>In compliance with our Data Security and Protection processes, all of Damibu's projects undergo a DPIA.<br>CATCH is commissioned by public sector organisations including NHS commissioning groups which is why we identified the need to complete a data protection impact assessment. |

## Step 2: Describe the processing

**Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Personal Data

This subdivided in to two forms:

Location – A user is asked for their Post Code so they can be assigned to the correct Local Authority / Clinical Commissioning Group (LA/CCG) area. This information is sent securely via SSL to the cloud-based CATCH platform. The CATCH system uses this information to calculate the LA/CCG area and return back Location Data containing, Postal District, NHS LOSA and Ward. This Location Data is sent with every Usage Event – described below.

Children – A user can add multiple children to the app by defining their name, gender and date-of-birth. This Children Data is used to highlight relevant health information articles to the user and is never transmitted from the app.

Location and Children Data is held encrypted within the App’s database.

Usage Data

Usage Data is collected anonymously via Google Analytics and a bespoke system within the cloud-based CATCH platform hosted by Amazon Web Services. Usage Data is made up of discrete Usage Events such as the user reading a health information article.

Google Analytics and the bespoke system are only accessible by a limited number of Damibu employees. Data or reports may be shared with NHS organisations to identify any trends such as popular health topics.

There is no processing involved that could be identified as high risk.

**Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Personal Data
All CATCH app users can add any number of children. Adding Children Data is optional, however some functionality will be limited if it is not provided.  All Children Data will remain indefinitely until removed by the user which they can do at any time.

Adding Postal District is optional but if not added then the user must manually select their LA/CCG area.  If the user does add their Postal District they can later remove this information, in which case their User Events will not be assigned to any Location Data.

Usage Data

Usage Data covers: article opening and reading; app opening and closing; LA/CCG area; the act of adding/removing a child but no Children Data; search text;etc.  No confidential, personally identifiable information, special category or criminal offence data is collected.

Usage Data is stored indefinitely.

| |
|---|
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| The CATCH app can store personal information regards a user's children. At no point does this information leave the user's device, therefore it can not be accessed by any other party. The child's date-of-birth is used to highlight age related articles. Their name and gender is used to identify them to the user when highlighting the articles.<br>As personal information does not leave the user's device, no personal information about the users of CATCH is held in any external systems. Therefore, all Usage Data collected is anonymous and any requests for deletion or copies of data held about specific users cannot be fulfilled. |

| |
|---|
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
| Anonymous usage data is collected for the purposes of improving the product and recognising trends. Such as to understand exactly how the app is used, for what purposes, which sections are most often accessed, which articles are most often read and which issues are most commonly encountered. |

## Step 3: Consultation process

**Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Extensive information, with in the privacy policy, help section and as part of the onboarding process, is provided to the user on what data is collected and how it is used.

The app encourages users to directly contact Damibu to share their views or provide any feedback. A form on the website allows users to anonymously send messages to Damibu.

Commissioning organisations are consulted about the use of data prior to launching in a region.

External organisations such as ORCHA are consulted regularly to evaluate the app which includes how data is used and collected.

## Step 4: Assess necessity and proportionality

**Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Data is anonymised on the device before it is collected, preventing any possibility for misuse. The app provides extensive information to inform users on what anonymised data is collected and what it is used for.

## Step 5: Identify and assess risks

| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|---|---|---|---|
| 1. The data storage platforms are compromised.<br>2. Malicious code is inserted into the app and reuploaded to the distribution stores allowing for third parties to collect data.<br>3. A personal device is lost or stolen containing personal data. | Remote<br>Remote<br>Remote | Minimal<br>Severe<br>Minimal | Low<br>Low<br>Low |

## Step 6: Identify measures to reduce risk

| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
|---|---|---|---|---|
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| 2. | The app is distributed through the Google / Apple and any code changes are signed with a private key which are stored offline so third parties cannot update products with malicious code even if they had access to Damibu's Google / Apple Account. | Reduced | Low | Yes |

# Step 7: Sign off and record outcomes

| Item | Name/position/date | Notes |
|---|---|---|
| Measures approved by: | John Callaghan, SIRO, 28th March 2019 | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | John Callaghan, SIRO, 28th March 2019 | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | Maja Lorkowska, DPO, 28th March 2019 | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: The DPO had no further comments. | | |
| DPO advice accepted or overruled by: | John Callaghan, SIRO, 28th March 2019 | If overruled, you must explain your reasons |
| Comments: None | | |
| Consultation responses reviewed by: | N/A | If your decision departs from individuals' views, you must explain your reasons |
| Comments: None | | |
| This DPIA will be kept under review by: | Maja Lorkowska, DPO | The DPO should also review ongoing compliance with DPIA |