

# DPIA for Tooth Fairy audit

---

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

## Step 1: Identify the need for a DPIA

**Explain broadly what the 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.

### *Aims of project*

Tooth Fairy Services is a specialist, UK-wide NHS service, within Paediatric Happiness Services in the UK to collect Baby Teeth as they naturally fall out. Tooth Fairy Services safely destroys these Baby Teeth so that children are guarded against any malign influences, as it is thought that if a third party obtains a child's baby teeth it can gain undue influence over the happiness of that child. When the Tooth Fairy collects the teeth from each child she leaves a small remuneration in the form of money or a gift, the value of which is determined by the child's family.

In January 2012, Tooth Fairy Services introduced the PilloWapp™ developed by Puck Enterprises, which detects when a child puts a tooth under a pillow for the Tooth Fairy, the location of the tooth to be collected and coded child identifiers (name, TFS ID number and NHS number/CHI number in Scotland). Prior to 2012, Tooth Fairy Services relied on household fairies to convey the information. The data retained by the PilloWapp™ includes coded patient identifiers, location information and the current family level of remuneration; these data are used only for the collection of teeth. The PilloWapp™ does not collect data regarding dental health of any children. The PilloWapp™ data are protected by Strong Magic during the data-transfer and Tooth Fairy Service provision. Once the tooth has been collected, the PilloWapp™ data are transferred and stored in a child-specific data file and held securely at Tooth Fairy Services HQ, located in central Nowhere, UK.

To determine the effectiveness of the PilloWapp™ and to identify any areas for improvement, Tooth Fairy Services needs to be audited with regard to the uptake of the service among children, the different factors that might affect service use or provision, and whether the introduction of the PilloWapp™ has affected these. Differences in remuneration will also be assessed with a view to standardisation across the UK.

We wish to audit/evaluate Tooth Fairy Services, comparing the 5 years before and after the introduction of the PilloWapp™, using data linkage to external Dental data to determine:

1. The level of use of Tooth Fairy Services across the UK, compared with the number of

- children, aged 5–15 years, registered with an NHS Dentist;
- a. Whether introduction of the PilloWapp™ affected service uptake using a ‘before and after’ analysis;
  - b. Whether specific social and geographical factors, might affect service coverage or use of the PilloWapp™;
2. Whether the health of the teeth and/or any dental intervention in its extraction affect the ability of the PilloWapp™ to detect teeth that should (or not) have been collected;
    - a. As above, whether this is affected by specific social or geographical factors;
  3. The variations in monetary remuneration across the service
    - a. Whether this is affected by specific social or geographical factors
    - b. Whether this has changed over time.

Results from this audit will be used to identify areas where service improvement may be required and possible factors that might affect the uptake or efficiency of the services. Differences in levels of remuneration, and the influence of social or geographical factors, will inform the ease of standardisation and the possible remuneration level that could be used for this standardisation.

#### *Type of processing involved*

The work will involve carrying out large scale processing of personal data and special category data:

- The personal data will be NHS / CHI number, name, address and date of birth;
- Special category data will be Dental health records and ethnicity.

The work involves data linkage between data collected by Tooth Fairy Services and Dental health data from the UK. The processing will include all children aged 5 to 15 years in the UK registered with an NHS dentist. These numbers will be compared with the number of children who have used Tooth Fairy Services to determine the level of uptake of Tooth Fairy Services. The processing will cover data from 2007 to 2017.

Processing for data linkage will be done by the data providers. For those children known to the Tooth Fairy, Tooth Fairy Services will provide the personal identifiers and receive back pseudonymised data. For those children who have not used the Tooth Fairy, no identifiers will be given to Tooth Fairy Services and the data will therefore be anonymised.

## 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 another way of describing data flows. What types of processing identified as likely high risk are involved?

### *Collection, use, storage and deletion of data*

Data relating to all children that have used Tooth Fairy Services are pseudonymised and stored separately from the child identifiers, which are retained securely for 20 years for collation of data for subsequent tooth collections. For further information regarding our service, please see our website: [www.toothfairy.service.uk](http://www.toothfairy.service.uk).

In January 2012, Tooth Fairy Services introduced the PilloWapp™ developed by Puck Enterprises, which detects when a child puts a tooth under a pillow, the location of the tooth to be collected and identity of the child identifiers (name, TFS ID number and CHI number). Prior to 2012, Tooth Fairy Services relied on household fairies to convey the information. The data retained by the PilloWapp™ includes coded patient identifiers, location information and the current family level of remuneration; these data are used only for the collection of teeth. The PilloWapp™ does not collect data regarding dental health of any children. The PilloWapp™ data are protected by Strong Magic during the data-transfer and Tooth Fairy Service provision. Once the tooth has been collected, the PilloWapp™ data are transferred and stored in a child-specific data file and held securely at Tooth Fairy Services HQ, located in central Nowhere, UK.

*What is the source of the data? You might find it useful to refer to a flow diagram or another way of describing data flows.*

We wish to audit/evaluate Tooth Fairy Services, comparing the 5 years before and after the introduction of the PilloWapp™, using data linkage to external NHS Dental data.

The audit will compare linked Tooth Fairy Services data prior to and subsequent to the introduction of the use of PilloWapp™. These data will be linked to the child dental data by personal identifiers (which will only be used for processing) and child-level study data will be pseudonymised using a study ID for analysis. Dental data for children who have not used the Tooth Fairy Services will also be obtained and given a different study ID by eDRIS. These children will be used in all analyses as a comparator group. Inequalities within the service will be analysed according to age and sex of the child, social deprivation, ethnicity, geography (postcode sector) and dental health to identify whether these have arisen in a systematic manner.

*Population:* All children (aged 5-15 years) known to Dental Services in the UK between 2007 and 2017. In 2014 the population of children within the UK was estimated to be ~7.4 million children. All those who have used Tooth Fairy Services will be linked with Dental health data. For those children who have not used Tooth Fairy Services, the same variables will be extracted and given new ID numbers. This will be the comparison group. Data from all children will be anonymised before returning to Tooth Fairy services.

**Intervention:** The audit will compare the use of Tooth Fairy Services across the whole UK, before and after the introduction of the PilloWapp™. As the PilloWapp™ was introduced in January 2012, data from 2007–2011 and 2012–2017 will be compared, as ~5 years either side of an intervention. Variations in service use over time will also be analysed according to age and sex of the child, social deprivation, ethnicity, geography (postcode sector) and dental health. Variations in remuneration over time will be analysed according to age of the child, social deprivation, ethnicity, geography (postcode sector) and dental health.

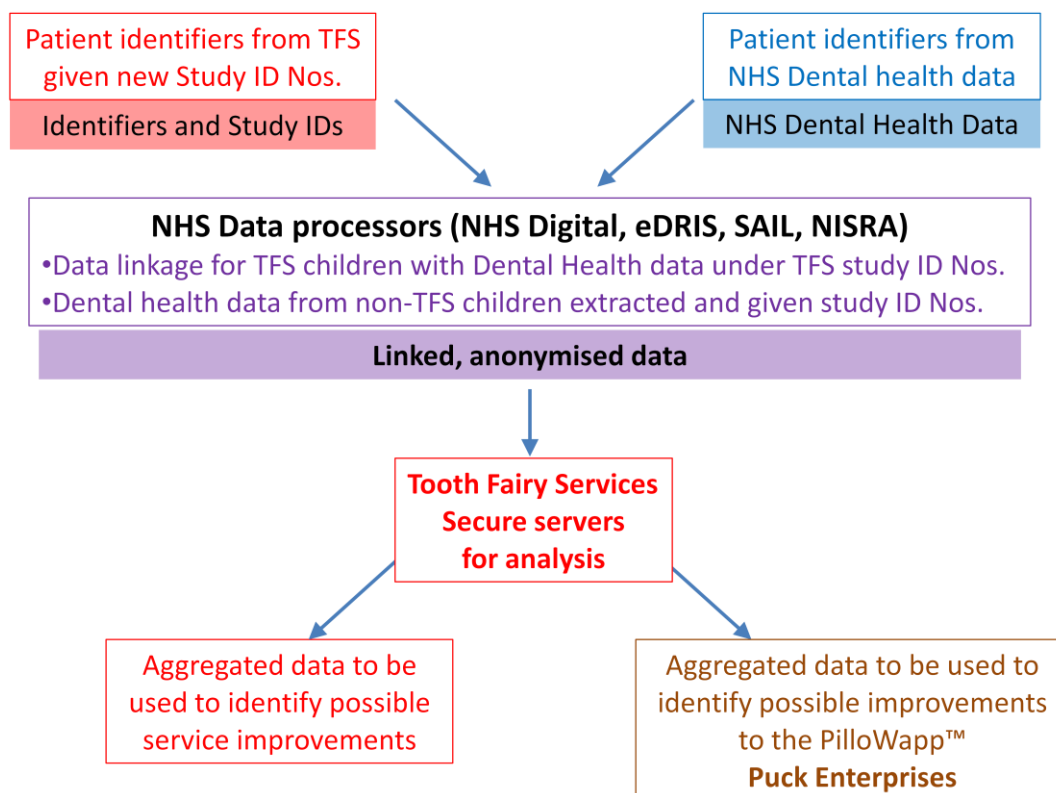
**Comparators:** Children who have not used Tooth Fairy Services will be the comparator group. Children who have and have not used the Tooth Fairy Services will be compared over the same time period. Differences over time will be analysed according to age and sex of the child, social deprivation, ethnicity, geography (postcode sector) and dental health.

**Outcomes:** population statistics between the groups.

#### Data Linkage

The data linkage between Tooth Fairy Services data and NHS Dental data will be carried out by the data providers: NHS Digital in England, the electronic Data Innovation Service (eDRIS) in Scotland, the Secure Anonymised Information Linkage (SAIL) Databank in Wales, and the Northern Ireland Statistics and Research Agency (NISRA) in Northern Ireland. Applications for access to Dental Health data and the data linkage process will be submitted to each of the appropriate agencies.

#### Flow diagram:



### Data flow

Patient identifiers held by Tooth Fairy Services and a study-specific TFS ID number will be sent to the NHS Data providers for each part of the UK (England, Scotland, Wales, Northern Ireland). Dental data will be provided by the providers and linked to the study-specific ID number by the NHS Data providers. The data and TFS ID number will be returned to Tooth Fairy Services where it will be held on secure services. This is pseudonymised data as Tooth Fairy Services still hold the identifiers, but these will be kept completely separately.

Data from control children: those registered with an NHS dentist but who have never used the Tooth Fairy Services will be given a different study ID number by the NHS Data providers and the data sent to Tooth Fairy Services. These data will be anonymised data as Tooth Fairy Services will have no access to any identifiers for these children.

All data will be pseudonymised / anonymised for analysis. All data will be stored and analysed on secure Tooth Fairy Services servers located in central Nowhere.

#### *What types of processing identified as likely high risk are involved?*

The large volume of data required for the audit increases the level of risk for processing. Therefore, using a data linkage strategy, whereby the data providers extract and link the data to the TFS identifiers and return pseudonymised data, reduces that level of risk. Data from children who have not used Tooth Fairy Services will be extracted and anonymised by the data providers and returned as an anonymised dataset.

#### *Will you be sharing data with anyone?*

De-identified, aggregated data will be used by Puck Enterprises (inventors of the PilloWapp™) and by the Service Improvement team of the Tooth Fairy Services, to determine if the PilloWapp™ or Tooth Collection can be improved.

**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?

#### *What is the nature of the data, and does it include special category or criminal offence data?*

The audit will include personal and special category data from children.

**Personal data** from children will be: name, address, NHS/CHI number, postcode will be used for processing only.

Data will be pseudonymised by using a unique Tooth Fairy study ID number for each child, which will be different from the Tooth Fairy Services ID.

**Special category data** will be: Dental health data and ethnicity.

No criminal offence data will be requested.

#### *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?*

Tooth Fairy Services covers children across the UK. The level of uptake of Tooth Fairy services is unknown and is one of the questions to be determined in this audit.

The data requested and analysed will be dental health data from all children aged 5–15

years, from between 2007 and 2017, from across the UK. The population of children in the UK for the year 2014 was approximated to be ~7.4 million children.

Once the audit has been completed the pseudonymised data will be securely stored for 20 years, according to the retention policies of Tooth Fairy Services, while the personal identifiers will be destroyed. Only aggregated will be reported in internal documents and on the Tooth Fairy Services website and used for informing area for service improvements.

**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)?

*What is the nature of your relationship with the individuals? How much control will they have?*

The data held by Tooth Fairy Services was obtained from each occasion that a child put a tooth under a pillow for collection by the Tooth Fairy. These data were all from children within the UK, and might have included some who were from vulnerable groups but these were not have been identified or targeted.

For service provision, Tooth Fairy Services has to collect name and address of each child, to ensure that the right tooth is collected and to prevent wasted journeys due to confusion of identity. The PilloWapp detects and protects the presence of a tooth by Strong Magic, but the collection of the tooth is still done by specific collection fairies. There is no compulsion for anyone to use Tooth Fairy Services.

The rights of the individuals will be upheld:

- Right of access: Subjects have right to access their data. Tooth Fairy Services have processes in place to respond to Subject Access Requests.
- Right to rectification: Tooth Fairy Services collect data that is correct at the time of tooth collection. Should this information subsequently change (e.g. child has changed name or address), the information obtained may be updated in the Tooth Fairy Services database for future use, but the record from the time of the tooth collection will remain, as it was correct at the time of collection.
- Right to object: The individual has the right to object to processing of their data by Tooth Fairy Services and be removed from the system. However, if subsequent to their objection, they activate the PilloWapp™, by placing a tooth under a pillow for collection by the Tooth Fairy, their new data will be processed accordingly.
- Right to restrict processing: The individual has the right to restrict processing of their data by Tooth Fairy Services and be temporarily restricted within from the system, for a mutually agreed period of time. Restriction will be done by flagging the data on the system to prevent it from being processed. However, if, subsequent to this restriction, they activate the PilloWapp™ by placing a tooth under a pillow for collection by the Tooth Fairy, their data will be processed accordingly.
- Right to data portability: This right does not apply, as the lawful basis for processing data

by Tooth Fairy Services is not consent, or the performance of a contract, and the data is not processed by automated means.

- Right to erasure: The individual has the right to have their data erased from the Tooth Fairy Services and be removed from the system. However, if subsequent to their erasure, they activate the PilloWapp™ by placing a tooth under a pillow for collection by the Tooth Fairy, their new data will be processed accordingly and a record will be made. Records are removed from the system after 20 years.
- Rights in relation to automated decision-making and profiling: Data processing within Tooth Fairy Services does not include automated decision-making and profiling.

*Would they expect you to use their data in this way?*

During 2018, Tooth Fairy Services carried out some public surveys at several locations around the UK, to ask the general public about their use of Tooth Fairy Services and what they thought of the use of their/their children's de-identified data for analysis to identify service improvements. The results indicated that the Public were supportive, with ~91% agreement.

Please see attached analysis of Tooth Fairy Services Public Engagement.

*Do they include children or other vulnerable groups?*

Tooth Fairy Services collects data from children within the UK, which might include some who were from vulnerable groups but these were not identified or targeted.

*Are there prior concerns over this type of processing or security flaws?*

No.

*Is it novel in any way?*

Tooth Fairy Services is the only provider of services for the Tooth Fairy. Because of the potential vulnerability of the children being served, when Tooth Fairy Services was set up, it was felt that a UK-wide service within the NHS Paediatric Happiness Services, would be a more efficient way to ensure national coverage.

*What is the current state of technology in this area?*

The PilloWapp™ is the most recent technological advancement in this area and the purpose of this study is to audit its performance pre- and post-introduction.

*Are there any current issues of public concern that you should factor in?*

None for which we have been notified in our public surveys.

*Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?*

All Fairies employed by Tooth Fairy Services must be registered members of the General Fairy Council.

**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?

*What do you want to achieve?*

We wish to audit/evaluate the Tooth Fairy Service to determine the effectiveness of the

PilloWapp™, comparing the 5 years before and after the introduction of the PilloWapp™, using data linkage to external Dental data. In addition we wish to identify any areas for improvement for Tooth Fairy Services, the different factors that might affect service use or provision, and whether the introduction of the PilloWapp™ has affected these. Differences in remuneration will also be assessed with a view to standardisation across the UK.

*What is the intended effect on individuals?*

The intended effect on individuals is a more efficient service for children, and more efficient use of Tooth Fairy Services resources.

*What are the benefits of the processing for you, and more broadly?*

The benefits of processing is to obtain an accurate picture of the extent of the UK coverage of the Tooth Fairy Services, as determined by the proportion of children who have used the service in those registered with NHS Paediatric Dental services. Investigation of the social and geographical factors that might affect service uptake will determine the areas where service provision can be improved.

## 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?

*Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.*

Children show their awareness of Tooth Fairy visits by putting teeth under their pillow for collection by the Tooth Fairy. This information was detected and passed on by household fairies prior to the introduction of the PilloWapp™, which is meant to detect this information using StrongMagic. Privacy Notices regarding the use of child data obtained by Tooth Fairy Services are available on our website: [www.toothfairy.service.uk/privacy-notices](http://www.toothfairy.service.uk/privacy-notices).

During 2018, Tooth Fairy Services carried out some Public surveys from around the UK, to ask the general public about their use of Tooth Fairy Services and what they thought of the use of their own/their children's de-identified data for analysis to identify service improvements. The results indicated that the Public were supportive, with ~91% agreement.

*Who else do you need to involve within your organisation? Do you need to ask your processors to assist?*

There is a team of tooth collectors / analysts within the organisation, who are used to transcribing and analysing using the Tooth Fairy Service data and keeping records up to date. These are all trained in Information Governance and have signed confidentiality protocols held by the organisation.



*Do you plan to consult information security experts, or any other experts?*

Tooth Fairy Services data are stored on secure servers, located in central Nowhere. The data and outputs from this project will be stored on separate areas of these servers with separate access points and with a Dragon Firewall, which prevents the data from being accessed from the same areas in which the routine Tooth Fairy Service data is stored and maintained.

## 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?

*What is your lawful basis for processing?*

Legal basis for processing personal data:

**6.1.e:** Public task: the processing is necessary for the data controller to perform a task in the public interest or for their official functions, and the task or function has a clear basis in law.

Legal basis for processing special category data:

**9.2.g:** Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

*Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep?*

We believe the processing will not require further variables. For the audit, we do not believe there is another way of determining the level of uptake of Tooth Fairy Services without comparing our data with UK-wide data regarding registration of children with NHS dentists. We have requested a single transfer of data from specific dates from each NHS data provider within the UK.

*How will you ensure data quality and data minimisation?*

For data minimisation, dates have been reduced to month and year; postcode sector will be returned for geographical analysis; deprivation measures will be derived from full postcode by the data processors but the full postcode will only be used for processing and for assigning deprivation scores. By using data linkage, the data controllers will be providing the NHS data using their own service providers, thus ensuring data quality.

*What information will you give individuals? How will you help to support their rights?*

Children show their awareness of Tooth Fairy visits by putting teeth under their pillow for

collection. This information was detected and passed on by household fairies prior to the introduction of the PilloWapp™, which is meant to detect this information using StrongMagic. Privacy Notices regarding the use of child data obtained by Tooth Fairy Services are available on our website: [fww.toothfairy.service.uk/privacy-notices](http://fww.toothfairy.service.uk/privacy-notices) and (accompanying document).

For children who did not use the Tooth Fairy Services, information regarding use of health data for audit and service improvement is available on NHS websites. For children who did not use the Tooth Fairy Services, only anonymised data will be used, as Tooth Fairy Services have no personal identifiers for them and will not request any personal identifiers. At the end of the audit a report containing only aggregated data will be published on our website, disseminated to Paediatric Dental Services across the UK and used to identify possible improvements to Tooth Fairy Services or the PilloWapp™ device.

*What measures do you take to ensure processors comply?*

Data extraction from routine NHS data will be done by the NHS Data providers who will comply with their own policies and procedures. All data will be analysed within Tooth Fairy Services. All Tooth Fairy Services analysts sign confidentiality agreements according to the Tooth Fairy Services confidentiality policy prior to accessing the data. Access to all information systems will be controlled to ensure that only authorised users have access to the system and the information they are authorised to access. Tooth Fairy Services data systems have an audit functionality which records user access to confidential data items and keystroke use. Audit data will be used for review of actual or potential IG breaches/incidents. Routine audit of access will also be carried out. Where more than one user accesses an information system, each user of that system will have a unique and verifiable identity. All transactions on shared information systems will be attributed to the individual who initiated them.

Access to the data will be via Data Access Consoles from within the Tooth Fairy Services complex in central Nowhere. All access is from individual accounts which are password-protected. Passwords must be changed every full moon, and must include combinations of letters (higher and lower case), numbers, runes and symbols. All Data Access Consoles are monitored by keystroke analysis. Anti-virus, anti-malware software and Spell Checkers are installed on all data access consoles and these are updated daily.

*How do you safeguard any international transfers?*

All data will remain within the UK and will not be transferred overseas.

## Step 5: Identify and assess risks

<b>Describe the source of risk and nature of potential impact on individuals.</b> Include associated compliance and corporate risks as necessary.	<b>Likelihood of harm</b>	<b>Severity of harm</b>	<b>Overall risk</b>
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
<p><b>Safe People</b>            Access to all information systems will be controlled to ensure that only authorised users have access to the system and the information they are authorised to access. Tooth Fairy Services data systems have an audit functionality which records user access to confidential data items and keystroke use. Audit data will be used for review of actual or potential IG breaches/incidents. Routine audit of access will also be carried out. Where more than one user accesses an information system, each user of that system will have a unique and verifiable identity. All transactions on shared information systems will be attributed to the individual who initiated them. All accounts will be password-protected: All passwords have to be changed at the full moon, the dates of which are set as reminders in the system's calendar. All passwords must be of at least 16 characters long and must contain at least one of each of the following: upper and lower case letters, numbers, runes and symbols. No password or one similar can be repeated within a year of use. The system records previous passwords for one year for each user for compliance.</p> <p><b>Safe Places</b>            All data on secure servers will be accessed via password-protected access through secure Data Access Consoles, within Tooth Fairy Services, based in Titania Way, Oberon Town, Nowhere, UK. NO15 9WH. Access to the buildings is via ID card and buildings are monitored by Closed Circuit FairyVision.</p> <p><b>Safe Data</b>            For children known to Tooth Fairy Services, all data will be pseudonymised and identifiers will be</p>	Remote	Minimal	Low
	Remote	Minimal	Low

<p>stored securely and separately from the data before being destroyed. For children who have never used Tooth Fairy Services, all data will be anonymised and no identifiers will be sent.</p>			
<p><b>IT security</b>  The servers are hosted in air-conditioned, locked rooms with access granted only to authorised IT staff. Access to the building is via ID card and is constantly monitored by Closed Circuit FairyVision (CCFV), intruder alarms and fire detection systems. Separate backup servers are situated in a separate building on the other side of the Tooth Fairy Services campus, a distance of about half a league. Servers undergo daily updates of software to guard against known and newly released viruses and malware; this also includes a Spell Check function. The servers record all access to the systems for all personnel, including system administrators. Audit logs are configured to record any actions undertaken using administrator or elevated privileges. All audit logs are secured to protect from unauthorised modification. Any unauthorised access to servers at this level can be detected and the account and user are automatically frozen. Servers are backed up daily and the back-ups retained for one month, after which they are routinely and securely written over. The Tooth Fairy Services servers can be set to prevent unauthorised electronic copying of data. If this is attempted access accounts and user are automatically frozen. All users sign a confidentiality user agreement which prohibits copying of data using any other means without authorisation.</p>	Remote	Minimal	Low
<p><b>Risk of unforeseen data leak</b>  The above measures ensure that the risk of unforeseen data leak is deemed to be small.</p>	Remote	Minimal	Low
<p><b>Overall Privacy risk</b></p>	Remote	Minimal	Low

## Step 6: Identify measure 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
		Eliminated, reduced or accepted	Low, medium or high	Yes / no
None identified				

## Step 7: Sign off and record outcomes

Item	Name / date	Notes
Measures approved by:	Tinker Bell Head of Numbers	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Fairy Liquid Head of Information Governance	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided by:	Fairy Nuff Data Protection Officer	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: All measures in place and are reasonable and achievable.		
DPO advice accepted or overruled by:	Tinker Bell Head of Numbers	If overruled you must explain your reasons
Comments: None		
Consultation responses reviewed by:	Fairy Godmother Clinical Lead for Child Happiness	If your decision departs from individuals' view, you must explain your reasons
Comments: None		
This DPIA will be kept under review by:	Fairy Liquid (Head of IG) Fairy Nuff (DPO)	The DPO should also review ongoing compliance with DPIA