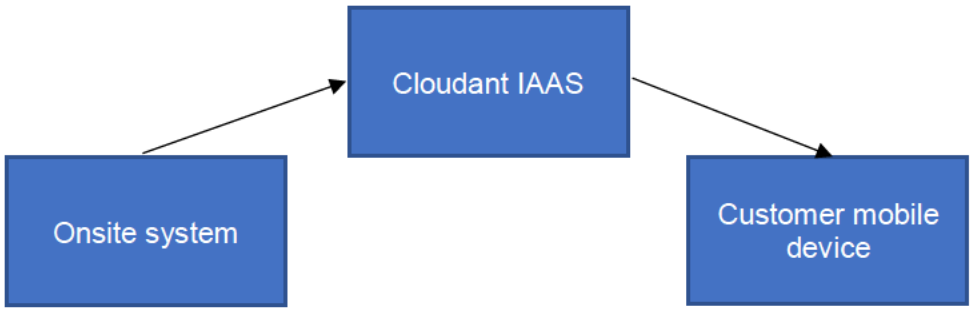
DPIA – Anywhere App/IBM Cloud Processing – InVentry Anywhere

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.
The aim of this project is to provide an improved user experience and increased functionality for the evacuation app, which forms parts of the InVentry sign in system. Currently the processing of the data for this is done within the services hosted by Rackspace in the UK, but to offer an increased efficiency to the application in terms of server processing speed and centralisation of IAAS it was decided to move the processing to IBM Cloudant services. The service offered by Rackspace does not allow the database to perform in a manner that provides the level of service required for the new application.

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?
The data is collected as part of the school/organisations signing in process using the InVentry signing in system. This data, identified in the list below, is transferred via https to the Anywhere cloud service for delivery to the mobile app. Once located on the Cloudant IAAS, the data is stored in an encrypted state. The data collected during the day is processed by InVentry until 23:59:59, at which point the current data is deleted and the process restarts for the following day. The data flow is described below:    The data is collected by the school/organisation and this original data is subject to the data retention policy of the organisation. The data processed by InVentry as described above is done so solely for the purpose of providing the evacuation service.

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?
The following data is processed as part of this service;

Staff – For use within the evacuation app
First name*
Surname *
Time signed IN*
Photograph (only if controller includes the field)
Position (only if controller includes the field)

Student – For use within the evacuation app (education only)
First name*+
Surname*+
Form group*+
Year group *+
Time signed IN*+
Time signed OUT*+
Reason for IN/OUT*+
MIS ID**+
AM/PM session mark**+

Visitor – For use within the evacuation app
Title*
First name*
Surname*
Company*
Photograph*
Vehicle registration*
Name of host/person visiting*
Time signed IN*

The Above fields marked with * are required for system functionality, fields marked with a ** are required if using the full MIS register function of the InVentry evacuation app. Fields marked with a + are not required for InVentry One systems.

No special category or criminal offence data will be transferred with the cloud service by design even if a customer chooses to keep such records in its own system.

The number of individuals will vary from site to site depending on the size of the site and the number of visitors.

The data is processed from the visitor on their arrival/departure and updated at that point to the Anywhere cloud service. Any data located in the cloud service will be deleted at 23:59:59

Currently the geographical areas for our product is as follows:
- UK
- EEA
- Middle East including United Arab Emirates
- Australia

It is currently not anticipated that this will expand beyond these regions in the foreseeable future.

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 relationship with the customer is one established via the contract (Article 6b) agreed when the customer purchases an InVentry system to manage their signing in or other services provided by InVentry Ltd. The data gathered from the individual data subjects is done under a legal obligation (Article 6c) placed on them or in performance of a task placed on them in the public interest (Article 6e). The individual will not have direct control over their data in the Anywhere system but they will be able to apply their rights via the customer who has the ability able to manage these via their unit console. The use of the data would be expected by the user for evacuation purposes. Depending on the level of integration with SIMs chosen by the controller in an educational deployment, the data described above of children would be processed but this is part of the service agreed with the school under contract. For commercial customers, there will be no child data. The organisation is currently undertaking Cyber Essentials accreditation.
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?
The introduction of the new InVentry app has required a change in cloud functionality. It has been designed from the ground up and will replace the existing evac and staff apps along with add extra functionality with a modern look and technical advancements. The new app allows you to do the following: • Pre-book your own visitors • View currently signed in staff • Perform an evacuation • Sign in to InVentry. This increased functionality has required the use of a more advanced web storage facility and this has been obtained via the move to IBM.

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?
The changes to the service have been led by suggestions from customers made via our help desk. These have been analysed by the development team and implemented accordingly. The development is an improvement to a current system and not a new implementation. For these reasons it was felt that there was no requirement for further consultation.

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?
The lawful grounds that InVentry undertake this processing is under GDPR Article 6b - processing is necessary for the performance of a contract to which the data controller has agreed. The data gathered from the individual data subjects is done under a legal obligation (Article 6c) placed on them or in performance of a task placed on them in the public interest (Article 6e). This is the responsibility of the customer. The processing will give increased functionality requested by the customers and could not have been achieved without this change due to the increased processing requirements. The ability to export the data to a form that can be used away from the system is currently available within the system in the form of a printed paper copy. However, this limits to point of access to a fixed device attached to the system and reduces the ability for the system to provide accurate data at the point of demand if required away from the system or attached fixed devices. The functionality is built within the app and any changes to alter this would require the development of a new app for the customers to download and use. Accuracy and management of the individual user rights are controlled by the controller/customer through their console and as such they remain responsible for this element. Where the customer is having an issue, InVentry Ltd will provide support to ensure the rights of the individual are met through its support desk. The customer will be informed of the changes through the release of this DPIA and notification of a change to the Privacy Statement. It will be the responsibility of the customer to inform the subjects within its control of such changes where it feels appropriate. InVentry cloud service is hosted by IBM on a Dedicated Hardware environment named "inventry001". The hardware is deployed to Softlayer datacenter in London GB and is covered under Article 45. This is also supported by the appropriate contracts (Article 46) and appropriate data sharing agreements which include standard data protection clauses as agreed by the commission (Article 93). The change of cloud service provider does not change any current status of services within the privacy and data sharing agreements Access to the data from the mobile app will be secured as described in Step 6 of this document.

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**
Exposure of personal data (adult) via system The impact on the data subject of the revelation of their personal data would have significant harm on their rights.	Possible	Significant	Medium
Exposure of personal data (child) via system The impact on the data subject of the revelation of their personal data would have harm on their rights.	Possible	Medium	Medium
Access to user system information by unauthorised processor obtained from user. If the user were to lose control of the device used to access the data, this could lead to data of individuals to be processed unlawfully and have significant impact on the rights of the data subject.	Possible	Significant	Significant

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**
Exposure of individual personal details during transfer and offsite (adult). Exposure of individual personal details during transfer and offsite (child).	Transfer between the onsite system, cloud storage and app is completed using https. Data centre discs are ‘at rest encrypted’. Additional security includes API access and IP Whitelisting. More details at: https://console.bluemix.net/docs/services/Cloudant/offerings/bluemix_dedicated.html#ibm-cloud-dedicated	Eliminated	Low	Yes

Access to user system information by unauthorised processor from user from	The app clears itself whenever the user logs out. Should the user not logout and simply 'kill' the app or leave it tabbed, the app only syncs data when active on the device (has focus) and requires device authentication (pin, fingerprint etc) before it can be re-opened. If by some means, the customer left the app fully open, because the app will sync with Cloudant at midnight when Cloudant clears itself, the device database will also be cleared. This means that should the device get lost or stolen, no data can be viewed.	Eliminated	Low	Yes

IBM Cloudant complies to the following recognised standards:

- IBM Cloud ISO 27001
- IBM Cloud ISO 27017
- IBM Cloud ISO 27018
- SOC 2 Type 2 Certification

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Adam Calvert 22/10/2018	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	David Tidman Data and Safeguarding Manager	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice: Customer should be advised that the use of the app is best done so on a device owned by the organisation and not a personally owned device. If the organisation choose to allow this, they should have clear guidance and expectations on device security and use.		
DPO advice accepted or overruled by:	David Tidman Data and Safeguarding Manager	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Phil Brooke Technical Director	If your decision departs from individuals' views, you must explain your reasons
Comments: As request was based on requests from users, no further consultations were undertaken.		
This DPIA will kept under review by:	David Tidman Data and Safeguarding Manager	The DPO should also review ongoing compliance with DPIA