DSPT information to assist care providers

Company name everyLIFE Technologies
Product name PASS

DSPT	Aproaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
1.2.1	Yes	Does your organisation have up to date policies in place for data protection and for data and cyber securityConfirm that your organisation has a policy or policies in place to cover: Data Protection, Data Quaility, Record Keeping, Data securityand, where relevant, network security.	Does your data processing agreement impact the care provider, if so please document your policy and the scope where it would affect the customer	Yes we have up to date Data Protection policies in place. Our Data Processing Agreement covers the arrangements in place pursaunt to Article 28 of the GDPR and outlines our obligations in processing data on behalf of the care provider, including security obligations and incident management.
1.4.1	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Please explain how your product manages and shares personal information	Data is stored on the cloud within Amazon Web Services (AWS) daa centre in London. In PASS, we operate a role based access control which determines the types of information a given role can access within the system.
1.6.1	Yes	Does your organisation's data protection policy describe how you keep personal data safe and secure?	Please explain how your product keeps personal data secure	The mechanism for protecting data is outlined within the Data Processing Agreement which is provided to each PASS customer. We follow industry best practice in terms of encryption of data in transit and at rest.
1.6.4	Yes	What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately? Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question.	Discuss with care providers the arrangements they should consider to minimise the risks if mobile phones are lost or stolen and offer advise as necessary.	Whist everyLIFE does not manage customer devices, we ensure the security of information by assigning each PASS user has a unique username and paasword. All data is stored on PASS is encrypted, offering further security to the information.
1.6.5	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data? This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the Information Commissioner's Office (ICO	Care providers complete their own DPIAs, however may wish to discuss the supplier DPIA relevant to the technology that they are implementing to determine items such as data flows and data transfers.	Please get in touch with your customer success representative if you would like to see a copy of our DPIA that we have completed for PASS.
1.6.6	No	If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	Does your product have any tools to manage BYOD devices? If so please document how this helps a customer	Not applicable for everyLIFEas we currently manage devices. However we do signpost PASS customers to ICO best practice guidance pertaining to BYOD and suggestions for maintaining security when implementing BYOD are discussed as part of onboarding.
1.7.4	Yes	Does your organisation have a timetable which sets out how long you retain records for?	Please document your data retnention criteria	Our standard retention schedule is in line with the Records Management Code of Practice, 2020. This is set out in our service Terms and Conditions which PASS customers receive upon signing up for PASS. If your obligations for data retention exceed those stated within our Terms please discuss with us so we can agree a suitable option for your service care type.
1.8.3		What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?	Please give the reverse of the question, explainined what they have implemented to mitigate risks, so the customer can rank them for all systems in use by them	We undertake annual penetration testing which is carried out by an independent third party CHECK accreditated provider.

DSPT information to assist care providers

Company name everyLIFE Technologies
Product name PASS

DSPT	Aproaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
4.1.2	Yes	Does your organisation know who has access to personal and confidential data through its IT system(s)?	Please document how your product provides access control and audit of this information	All authorised users of PASS have a unique username and must use password that follows our strong password rules. All amendments made by users within the system produce a digital signature meaning that there is an audit of users' access to the system.
4.2.5	Yes	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	If your product can assist in managing access rights then please explain here	Using the Administrator rights, access to the system can be revoked at any time. Each care provider can assign a 'super user' who can manage this locally
4.5.4	Yes	How does your organisation make sure that staff, directors, trustees and volunteers use good password practice? If your organisation has any It systems or computers it should provide advice for setting and managing passwords. Each person should havve thier .l;own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be "strong" i.e. hard to guess.	If your product can assist in managing password practice then please explain here	See above
6.1.5	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	Does your product have any tools to give visibility of who has accessed each individual data record?	PASS provides an audit of users accessing the system which may assist in providing visibility of when information was aceessed and by whom.
6.2.3	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions.	If you provide any of these devices then please explain any malware management included on them.	everyLIFE does not provide computers and other devices to care providers within their service offering.
7.1.2	No	Does your organisation have a business continuity plan that covers data and cyber security?	Please explain your business continuity plans for data and cyber security here.	We have business continuity plans in place for data and cyber security. Our arrangements for data and cyber securitys are availble to share with PASS customers. Please contact your customer success representative to obtain further information
7.3.1	Yes	How does your organisation make sure that there are working backups of all important data and information? It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them.	Please document your data backup process.	Our data back- up process is avaialble to share with PASS customers.Please contact your customers success representative to obtain further information
7.3.4	No	Are backups routinely tested to make sure that data and information can be restored?	Please document your data backup process.	Yes back -up are routinely tested to ensure that they are usable if required
8.3.5	Yes	How does your organisation make sure that the latest software updates are downloaded and installed It is important that your organisation's IT system (s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question.	Does your product have automated updates. If so, please document how this occurs, and how a customer can check which version they are running.	We make all PASS updates are made available to customers as soon as they are ready for release. We monitor uptake of software updates and if necessary will perform a forced upgrade to ensure that customers are operating the latest available software.
9.1.1	No	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?	Do you manage any WiFi routers for customers? If so, please explain how.	Not applicable for everyLIFE.

DSPT information to assist care providers

Company name everyLIFE Technologies
Product name PASS

DSPT	Aproaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
9.6.2	No	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people)	Cloud systems are designed to reduce the need to hold any data locally, using API's to directly connect cloud based analysis and document system without the need to expose data to local storage risks. However, where the supplier includes provision of removable devices, these should be appropriately proetcted using encryption and /other technical measures.	PASS is a cloud based solution and everyLIFE does not provide removable devices as part of its service offering
10.1.2	No	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Please give contact details here for the provider to include in their supplier list	Our contact details are available on our website
10.2.1	Yes	Do your organisation's IT system suppliers have cyber security certification Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace	Please confirm if you have cyber security certification	everyLIFE is accrediated with ISO 27001
		Has your organisation completed the DSPT?	Have you completed the DSPT , if so where do you display this ?	Yes. Confirmation of publication is available via the DSPT website organisational search
		GDPR statement and contract with supplier	Please give a link to your GDPR statement, ideally in as plain English/easy to understand format as possible	This is as detailed within our Data Sharing Agreement that is provided to all PASS customers