GDPR Systems

Office GDPR User Guide

November 2018

Helpdesk Tel:	01865 600 410
Helpdesk Email :	info@gdprsystems.co.uk

Contents

Checklist for OFFICE GDPR Solution

To help you fill out your OFFICE GDPR solution quickly and easily you will need to have to hand the following information:

Section	What Do I Need?
Company Locations	All Company Locations (inc Home workers if relevant)
Company Information	Name/Address(es)/ICO Registration Number
Personnel Information	Name(s)/Contact Details of all staff that have access to personal information – both Physical and Digital Access
Asset Register	A list of equipment that stores/transmits data
Routers	Name/Make/Model/Serial Number
VPN	Type of VPN
Storage	Name/Make/Model/Connection Type/Operating System/Encryption Details
Databases & Files	Filepath/Database Type/Version Number
Private keys	Type/Filepath
Certificates	All Details
Data Transfers (Inbound/Internal/Outbound)	Name of Data Transfer/Your purpose for using the data/The Personal Data used/Contracts authorising you to process the data/Filepaths (if known)

GDPR Systems OFFICE GDPR User Guide Introduction

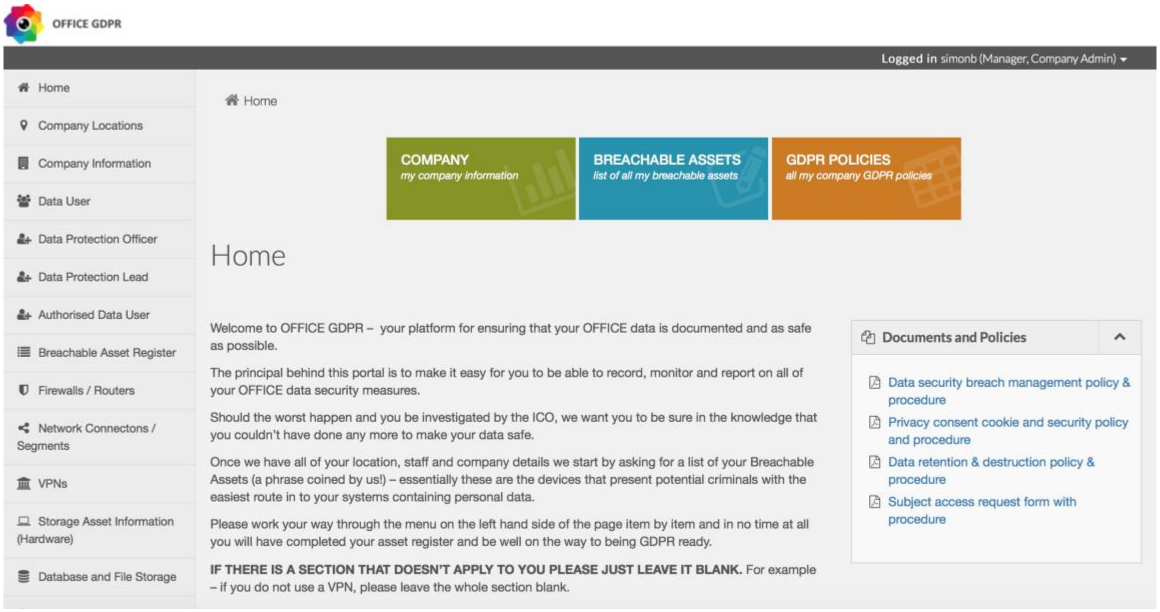
The following user guide explains the processes for your business to navigate and complete all sections of the GDPR Systems OFFICE GDPR solution.

You can access the GDPR Systems OFFICE GDPR solution here - portal.officegdpr.co.uk

Login using the Username and Password provided.

Use the contents page above to access any section within this document. Alternatively, you can go to any section of the guide using the headings listed down the left hand side of this document.
In addition, hyperlinks have been included throughout this User Guide to help you move to related sections within the document.

For further information, please contact the helpdesk either by phone on 01865 600 410 or by emailing info@gdprsystems.co.uk


OFFICE GDPR
Logged in simonb (Manager, Company Admin)
Home
Company Locations
Company Information
Data User
Data Protection Officer
Data Protection Lead
Authorised Data User
Breachable Asset Register
Firewalls / Routers
Network Connectons / Segments
VPNs
Storage Asset Information (Hardware)
Database and File Storage
Home
COMPANY
my company information
BREACHABLE ASSETS
list of all my breachable assets
GDPR POLICIES
all my company GDPR policies

Home

Welcome to OFFICE GDPR – your platform for ensuring that your OFFICE data is documented and as safe as possible.

The principal behind this portal is to make it easy for you to be able to record, monitor and report on all of your OFFICE data security measures.

Should the worst happen and you be investigated by the ICO, we want you to be sure in the knowledge that you couldn't have done any more to make your data safe.

Once we have all of your location, staff and company details we start by asking for a list of your Breachable Assets (a phrase coined by us!) – essentially these are the devices that present potential criminals with the easiest route in to your systems containing personal data.

Please work your way through the menu on the left hand side of the page item by item and in no time at all you will have completed your asset register and be well on the way to being GDPR ready.

IF THERE IS A SECTION THAT DOESN'T APPLY TO YOU PLEASE JUST LEAVE IT BLANK. For example – if you do not use a VPN, please leave the whole section blank.

Documents and Policies

- Data security breach management policy & procedure
- Privacy consent cookie and security policy and procedure
- Data retention & destruction policy & procedure
- Subject access request form with procedure

Purpose of the System

The OFFICE GDPR system has been designed to make it easy for you to be able to record, monitor and report on all of your Office personal data security measures.

Should the worst happen and you be investigated by the ICO, we want you to be sure in the knowledge that you couldn't have done any more to make your Office personal data safe.

The system consists of three main sections;

1. Company/Personnel Information: You will need to provide information about the people within your business.
   Who is responsible for data processes and security within the business?

2. Breachable Assets: You will need to list full details for all data related devices/items. Please note that this includes all forms of data e.g. paper based files and not just electronic devices.
   Who can access them?
   What happens to this information?

3. GDPR Policies: Completing the first two sections will populate the GDPR policies for your business, which can be stored and amended for future use, should you ever have GDPR related issue.

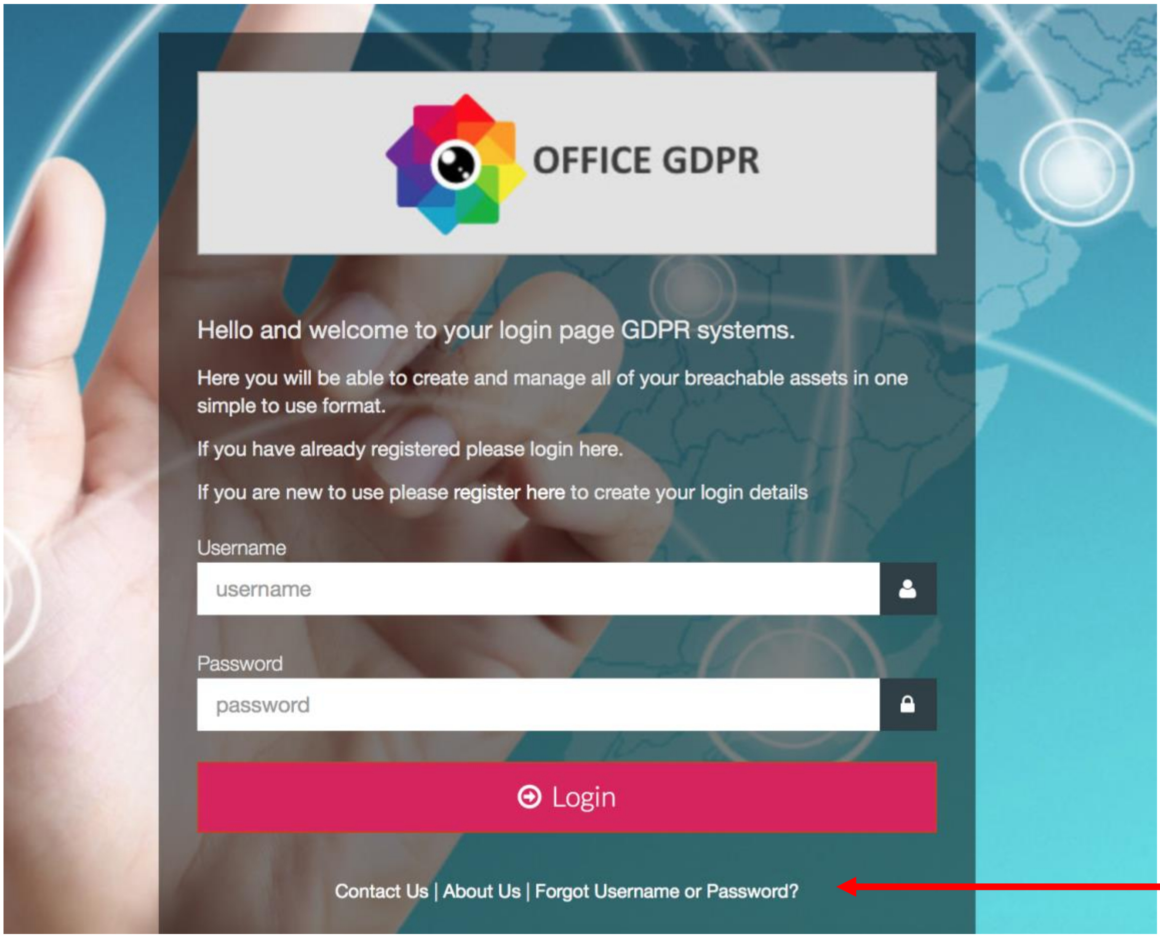
Login

Go to the URL portal.officegdpr.co.uk and enter your Username and Password into the respective fields and press the “Login” to log into the system.

Your Username is the email address used to set up your account.

Your Password will have been emailed to you as part of the initial welcome pack.

If you forget your password click “Forgot Username or Password” - located below the Login button - where you can request a new password to be sent to your registered email address. This is an automated service. You should receive your new password within one hour.



Hello and welcome to your login page GDPR systems.

Here you will be able to create and manage all of your breachable assets in one simple to use format.

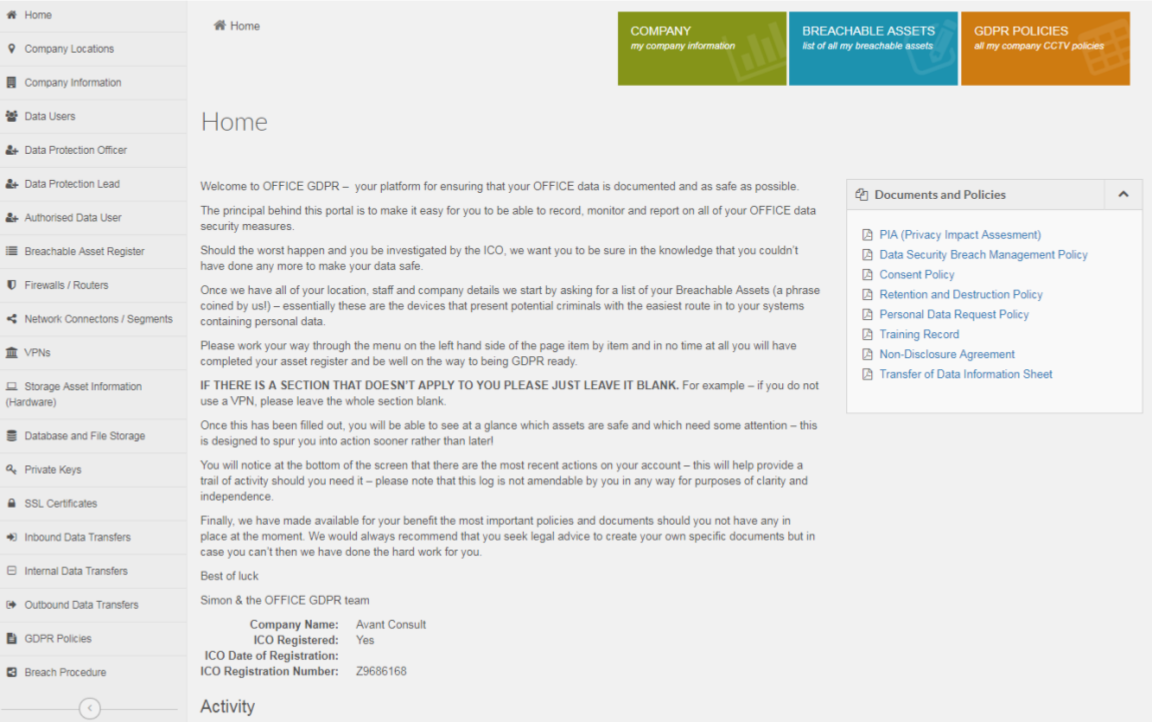
If you have already registered please login here.

If you are new to use please register here to create your login details

Once logged in, you will be directed to the “Home Page”.

Home Page

Once you have logged into the system you will be directed to the Home page, which provides some basic information for completing the required information, links to sections within the system, links to documents and policies and an "Activity Log" to show who has access the system, when and what has been done;



Home

Welcome to OFFICE GDPR – your platform for ensuring that your OFFICE data is documented and as safe as possible.

The principal behind this portal is to make it easy for you to be able to record, monitor and report on all of your OFFICE data security measures.

Should the worst happen and you be investigated by the ICO, we want you to be sure in the knowledge that you couldn't have done any more to make your data safe.

Once we have all of your location, staff and company details we start by asking for a list of your Breachable Assets (a phrase coined by us!) – essentially these are the devices that present potential criminals with the easiest route in to your systems containing personal data.

Please work your way through the menu on the left hand side of the page item by item and in no time at all you will have completed your asset register and be well on the way to being GDPR ready.

IF THERE IS A SECTION THAT DOESN'T APPLY TO YOU PLEASE JUST LEAVE IT BLANK. For example – if you do not use a VPN, please leave the whole section blank.

Once this has been filled out, you will be able to see at a glance which assets are safe and which need some attention – this is designed to spur you into action sooner rather than later!

You will notice at the bottom of the screen that there are the most recent actions on your account – this will help provide a trail of activity should you need it – please note that this log is not amendable by you in any way for purposes of clarity and independence.

Finally, we have made available for your benefit the most important policies and documents should you not have any in place at the moment. We would always recommend that you seek legal advice to create your own specific documents but in case you can't then we have done the hard work for you.

Best of luck

Simon & the OFFICE GDPR team

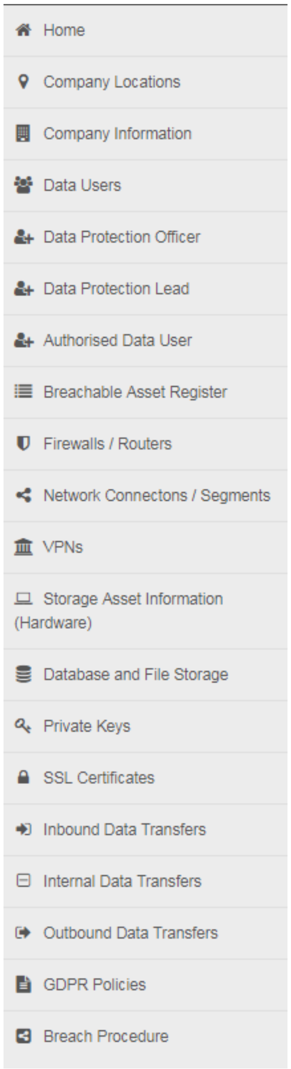
Company Name:	Avant Consult
ICO Registered:	Yes
ICO Date of Registration:	
ICO Registration Number:	Z9686168

Activity

Documents and Policies

- PIA (Privacy Impact Assesment)
- Data Security Breach Management Policy
- Consent Policy
- Retention and Destruction Policy
- Personal Data Request Policy
- Training Record
- Non-Disclosure Agreement
- Transfer of Data Information Sheet

Navigation



The GDPR Systems OFFICE GDPR system has been designed to be intuitive and user friendly, walking the user through the process of completing the required information in a logical and methodical fashion.

Once you have logged in you will see a navigation panel down the left hand side of the screen.

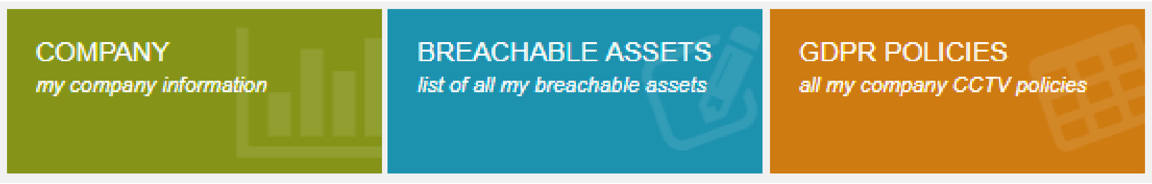
Click on any of the headings listed to go to the relevant section of the system. It is advised that you complete the sections in the order that they are listed in i.e. start at the top and work your way down.

While in the Portal you can use the back/forward arrows (← →) in the top left corner of your browser to move between previously viewed screens.

The system is comprised of three main areas;

1. Company Information:
   a. Locations data is used
   b. Data Users
2. Breachable Assets:
   a. Firewalls / Routers
   b. Network Connections / Segments
   c. VPNs
   d. Storage Asset Information
   e. Database and File Storage
   f. Private Keys
   g. SSL Certificates
   h. Inbound / Outbound Data Transfers
3. GDPR Policies

These main sections can also be accessed via the three coloured boxes in the top right of each page, as shown below:

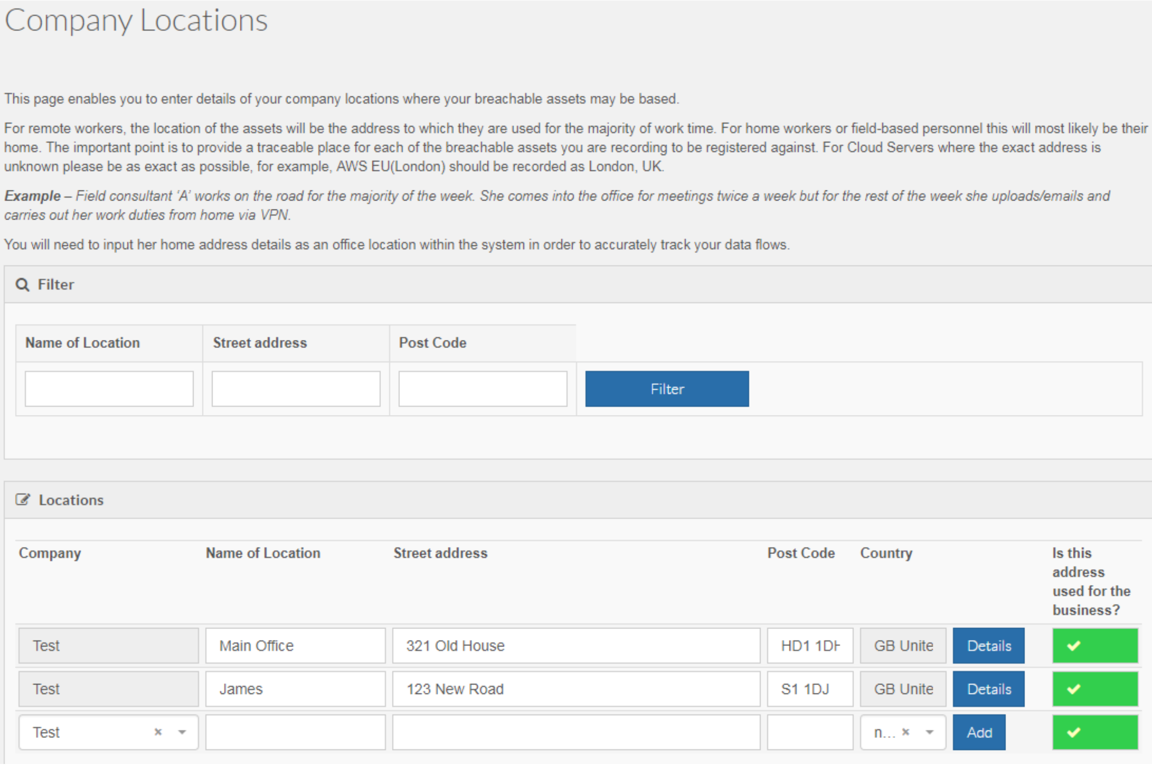

COMPANY
my company information
BREACHABLE ASSETS
list of all my breachable assets
GDPR POLICIES
all my company CCTV policies

Company Locations

In this section you will need to list basic information regarding the physical addresses where business data can be accessed. This will include your main site address but may also include the home addresses of staff if they are able to access work personal data remotely e.g. via a laptop or smart phone.

The first section provides a search facility to look up previously listed addresses. This can be useful if you have listed a large number of addresses related to the business.

The second section lists all the addresses logged so far. At the bottom of this section you can add (Add) addresses to your list. You can quickly create a list of locations with basic information from here by selecting a company (usually there will only be one option available), giving the location a name e.g. Head Office, a street address, postcode and country. Once complete, press the “add” button (Add) to add to the list. This basic information will then allow you to move onto the next section of the system, with the ability to add e.g. Users or Devices to this location. However, you will also need to complete further details about the location.



Company Locations

This page enables you to enter details of your company locations where your breachable assets may be based.

For remote workers, the location of the assets will be the address to which they are used for the majority of work time. For home workers or field-based personnel this will most likely be their home. The important point is to provide a traceable place for each of the breachable assets you are recording to be registered against. For Cloud Servers where the exact address is unknown please be as exact as possible, for example, AWS EU(London) should be recorded as London, UK.

Example *– Field consultant ‘A’ works on the road for the majority of the week. She comes into the office for meetings twice a week but for the rest of the week she uploads/emails and carries out her work duties from home via VPN.*

You will need to input her home address details as an office location within the system in order to accurately track your data flows.

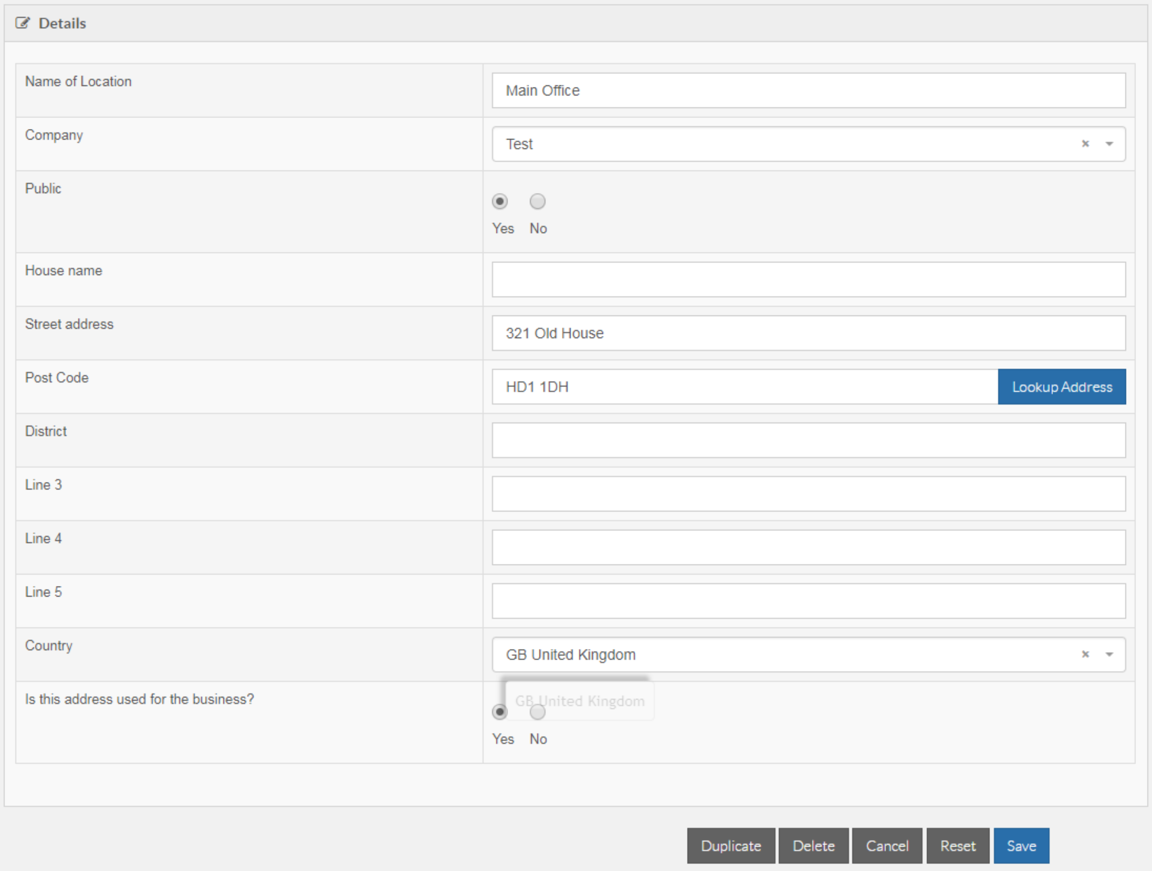
Filter

Name of Location	Street address	Post Code	
			Filter

Locations

Company	Name of Location	Street address	Post Code	Country		Is this address used for the business?
Test	Main Office	321 Old House	HD1 1DH	GB Unite	Details	✓
Test	James	123 New Road	S1 1DJ	GB Unite	Details	✓
Test ×				n... ×	Add	✓

To enter further details for a listed location, press the Details button (Details) to open the following screen:



Details

Name of Location	Main Office
Company	Test
Public	● Yes ○ No
House name	
Street address	321 Old House
Post Code	HD1 1DH
District	
Line 3	
Line 4	
Line 5	
Country	GB United Kingdom
Is this address used for the business?	● Yes ○ No

When entering the company address, simply input the postcode into the relevant field, press the “Lookup” icon (Lookup) and select the appropriate address. This will then populate the remaining address details. Alternatively, you can enter the information into each individual field.

Once you have completed all of the required information, please remember to click the “Save” icon (Save) at the bottom right of the page to save the data. **Moving away from the screen without saving will remove any changes you have made.**
If you wish to remove all data you can click the “Clear” icon (Clear) in the bottom right of the page.

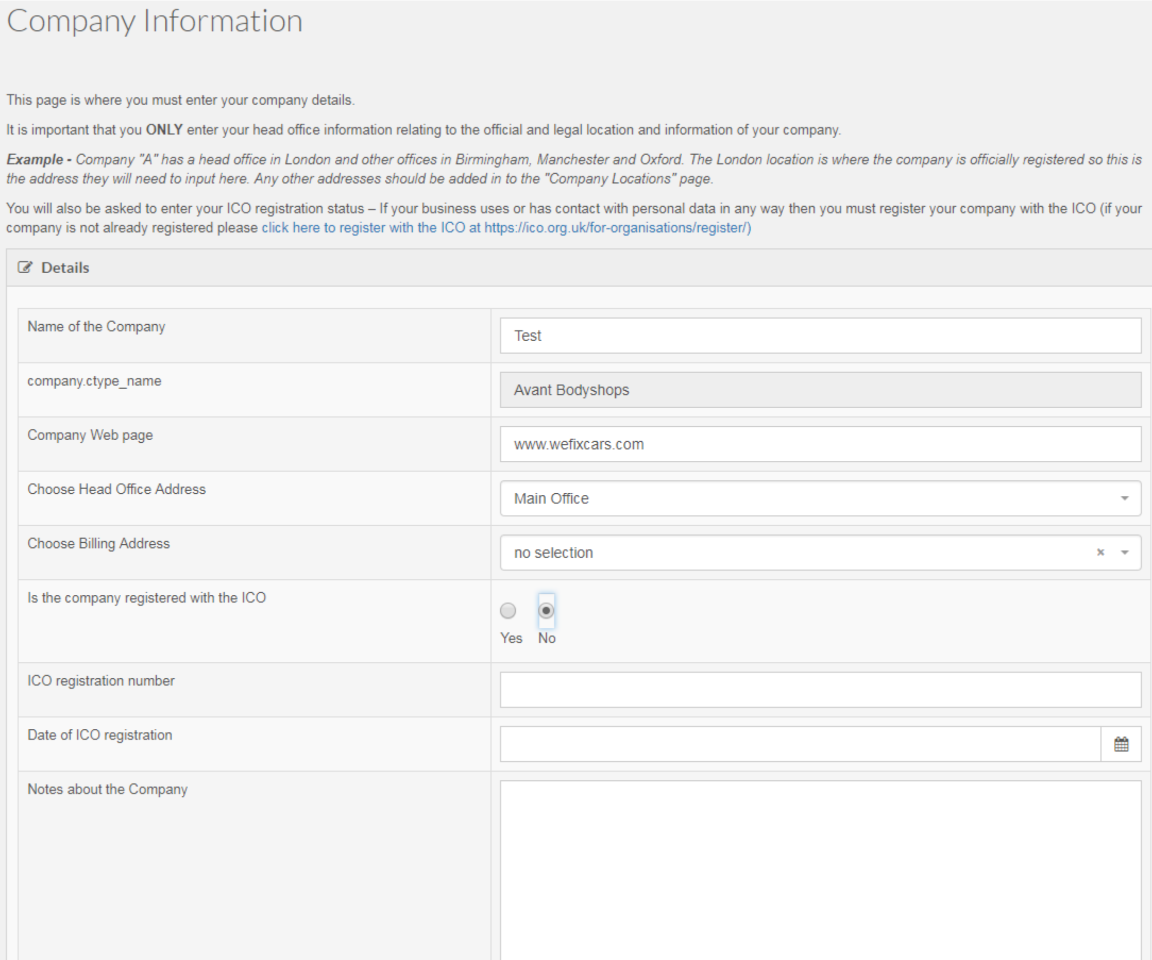
You will need to complete the full details for each of the locations listed.

Company Information

In this section you will need to complete details relating to your main site (head office). Please complete the information for all fields with a white background – those with a grey background are pre-populated.

For Head Office and Billing Address, you can select from the drop-down menu the locations you have listed in the previous section (Company Locations).

In this section you are also asked to include your ICO registration number. For businesses that are not registered with the ICO, a link has been provided for you to register, should you wish to do so.



Company Information

This page is where you must enter your company details.

It is important that you **ONLY** enter your head office information relating to the official and legal location and information of your company.

Example - *Company "A" has a head office in London and other offices in Birmingham, Manchester and Oxford. The London location is where the company is officially registered so this is the address they will need to input here. Any other addresses should be added in to the "Company Locations" page.*

You will also be asked to enter your ICO registration status – If your business uses or has contact with personal data in any way then you must register your company with the ICO (if your company is not already registered please click here to register with the ICO at https://ico.org.uk/for-organisations/register/)

Details

Name of the Company	Test
company.ctype_name	Avant Bodyshops
Company Web page	www.wefixcars.com
Choose Head Office Address	Main Office
Choose Billing Address	no selection
Is the company registered with the ICO	○ Yes ● No
ICO registration number	
Date of ICO registration	
Notes about the Company	

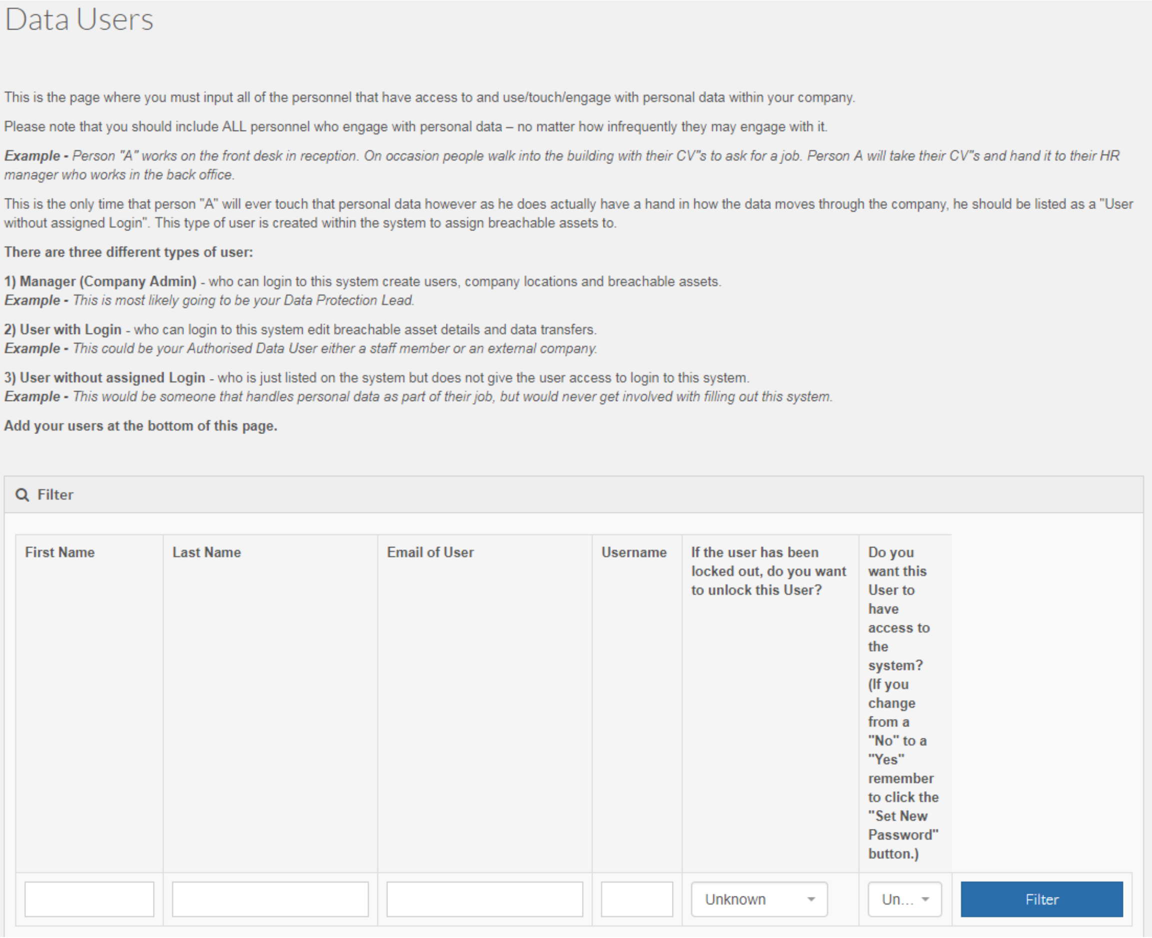
Data Users

In this section you will need to list all personnel who have access to data and data devices (administrative and physical access).

You are able to set up three types of user within the system;

- **Manager (Company Admin) –** these people have full access to the system, can edit data and create new users/devices
- **User with Login –** these people can access the system to update records relating to the asset register and data transfers
- **User without assigned Login –** these people engage with data or devices but are not required to access or enter information into this system

At the top of this section is a search facility (Filter). This will come in handy once you have created a full list of personnel.



Data Users

This is the page where you must input all of the personnel that have access to and use/touch/engage with personal data within your company.

Please note that you should include ALL personnel who engage with personal data – no matter how infrequently they may engage with it.

Example - *Person "A" works on the front desk in reception. On occasion people walk into the building with their CV"s to ask for a job. Person A will take their CV"s and hand it to their HR manager who works in the back office.*

This is the only time that person "A" will ever touch that personal data however as he does actually have a hand in how the data moves through the company, he should be listed as a "User without assigned Login". This type of user is created within the system to assign breachable assets to.

There are three different types of user:

1) Manager (Company Admin) - who can login to this system create users, company locations and breachable assets.
Example - *This is most likely going to be your Data Protection Lead.*

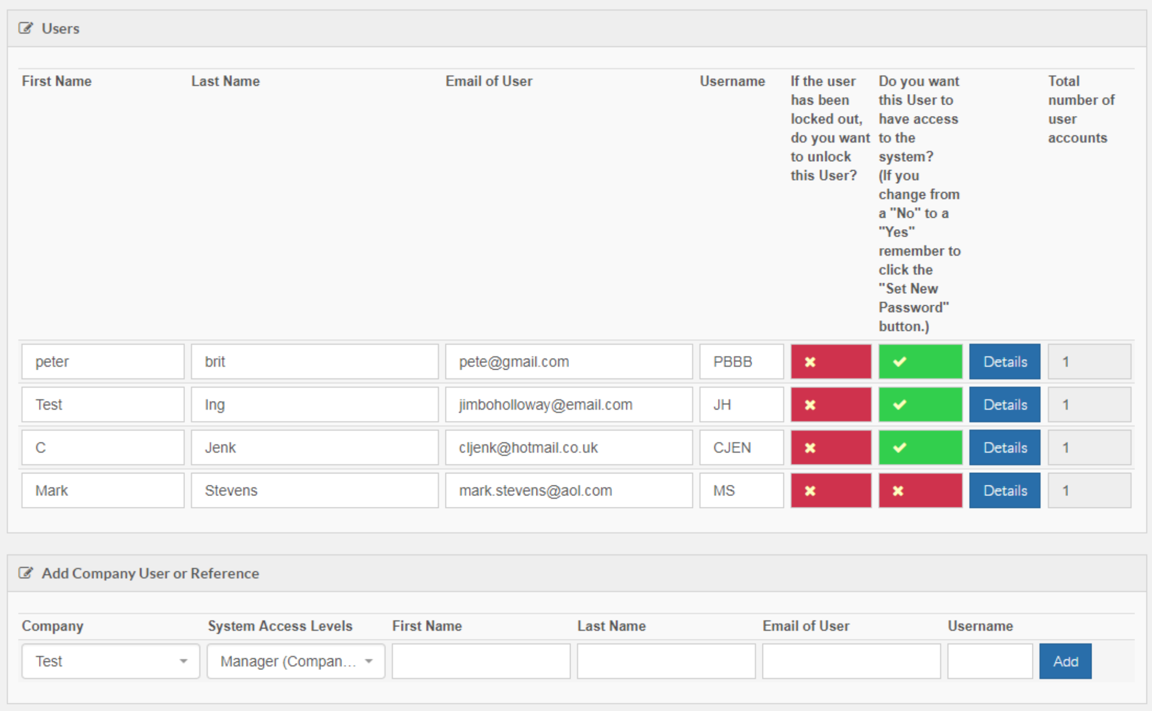
2) User with Login - who can login to this system edit breachable asset details and data transfers.
Example - *This could be your Authorised Data User either a staff member or an external company.*

3) User without assigned Login - who is just listed on the system but does not give the user access to login to this system.
Example - *This would be someone that handles personal data as part of their job, but would never get involved with filling out this system.*

Add your users at the bottom of this page.

First Name	Last Name	Email of User	Username	If the user has been locked out, do you want to unlock this User?	Do you want this User to have access to the system? (If you change from a "No" to a "Yes" remember to click the "Set New Password" button.)	
				Unknown	Un...	Filter

Below the search facility is a list of the data users you will have added. At the bottom of the screen you are able to add further data users.



Users

First Name	Last Name	Email of User	Username	If the user has been locked out, do you want to unlock this User?	Do you want this User to have access to the system? (If you change from a "No" to a "Yes" remember to click the "Set New Password" button.)		Total number of user accounts
peter	brit	pete@gmail.com	PBBB	✖	✓	Details	1
Test	Ing	jimboholloway@email.com	JH	✖	✓	Details	1
C	Jenk	cljenk@hotmail.co.uk	CJEN	✖	✓	Details	1
Mark	Stevens	mark.stevens@aol.com	MS	✖	✖	Details	1

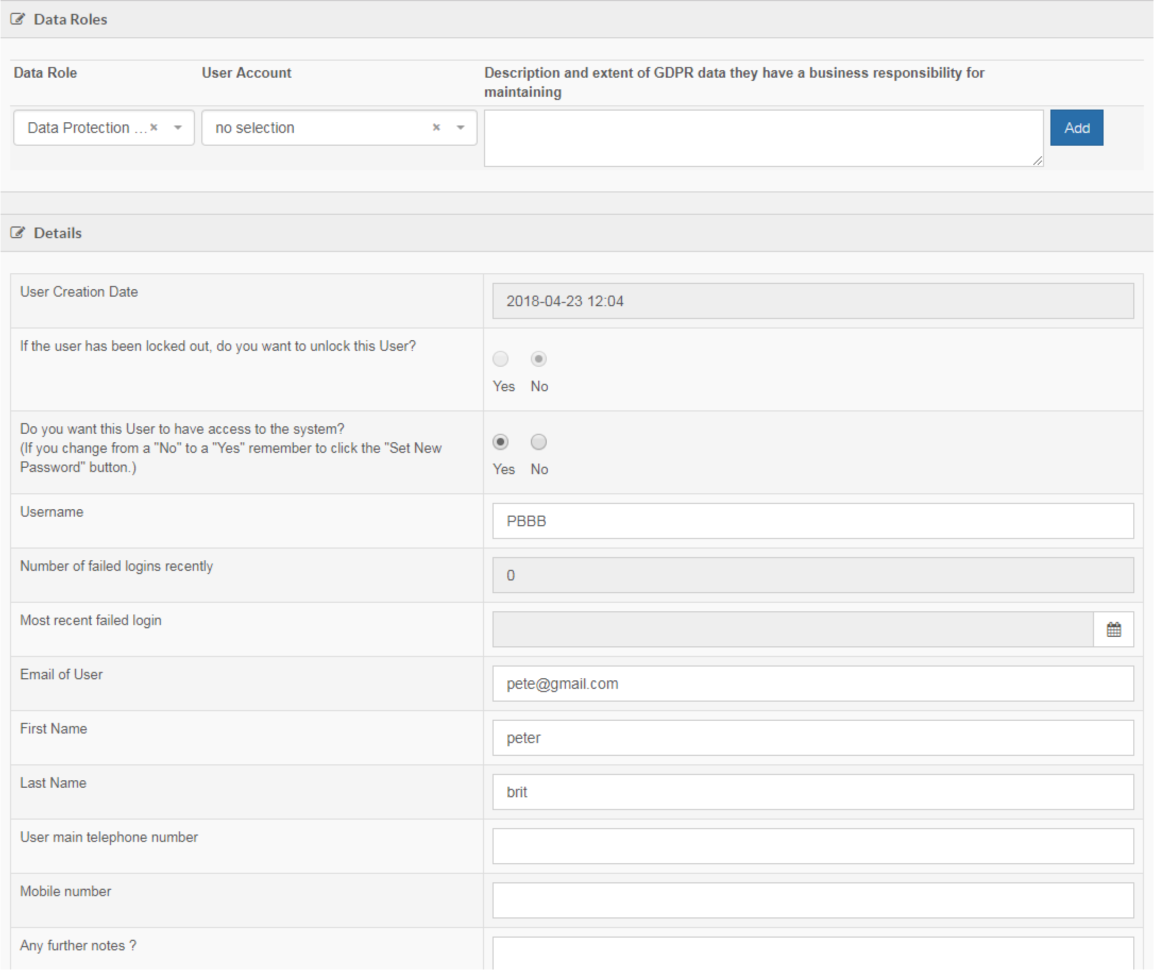
Add Company User or Reference

Company	System Access Levels	First Name	Last Name	Email of User	Username	
Test ▾	Manager (Compan… ▾					Add

To create a basic list of Data Users, select the company and chose a System Assess Level (from the three options listed above). Then enter their first and last names, their email address (this will be used to send them their password if you have selected an appropriate access level) and a unique user name (the user can use their email address or this username when logging into the system).

Once these details have been included, press "Add" (Add) to create the Data User.

Once a Data User has been added, you can click on their "Details" button (Details) to add further information about the user.



Data Roles

Data Role	User Account	Description and extent of GDPR data they have a business responsibility for maintaining	
Data Protection ... ×	no selection ×		Add

Details

User Creation Date	2018-04-23 12:04
If the user has been locked out, do you want to unlock this User?	○ Yes ● No
Do you want this User to have access to the system? (If you change from a "No" to a "Yes" remember to click the "Set New Password" button.)	● Yes ○ No
Username	PBBB
Number of failed logins recently	0
Most recent failed login	
Email of User	pete@gmail.com
First Name	peter
Last Name	brit
User main telephone number	
Mobile number	
Any further notes ?	

Please complete the information for all fields with a white background – those with a grey background are pre-populated.

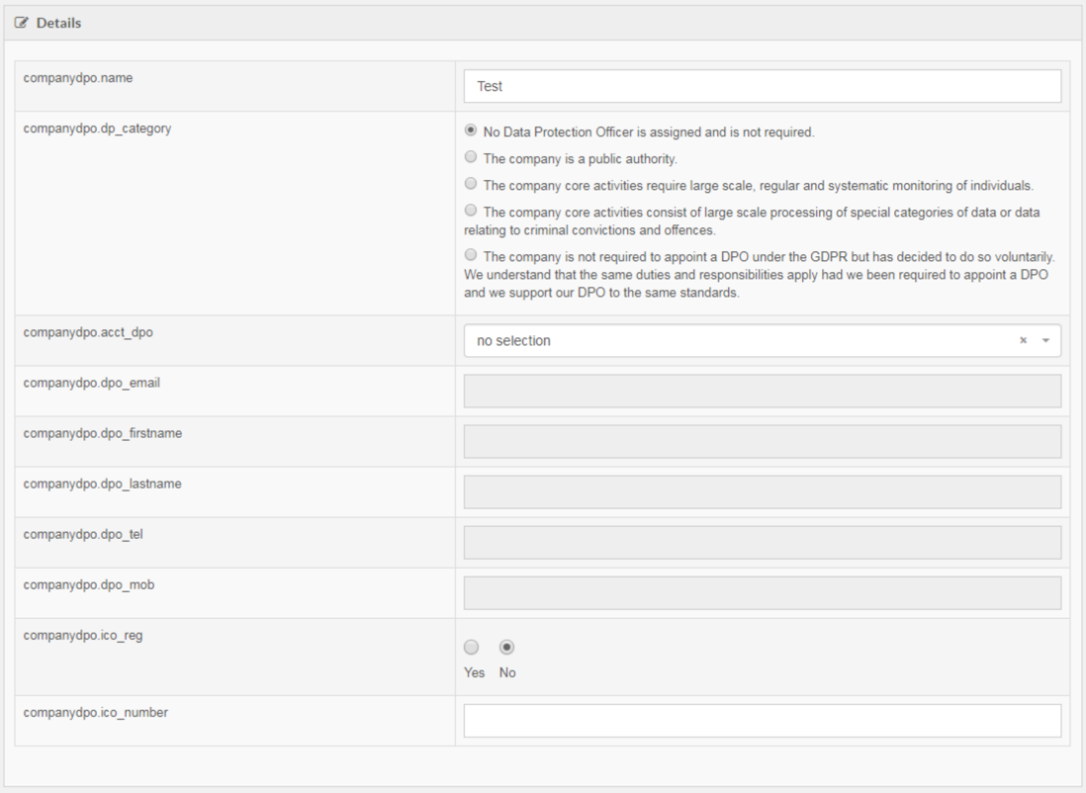
Data Protection Officer (DPO)

The Data Protection Officer is a formally recognised role which companies must employ providing they meet the required criteria. Even if a company doesn't meet the criteria it can choose to appoint a DPO.

The GDPR is explicit about the tasks that DPOs are required to perform. They include the following (Article 39):

- Inform and advise the organisation and its employees of their data protection obligations under the GDPR.
- Monitor the organisation's progress and readiness for the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes.
- Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting.
- Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

In this section you can select a DPO from your list of Data Users, or select from an appropriate answer from the list provided to state why you do not require a DPO. .



Details

companydpo.name	Test
companydpo.dp_category	● No Data Protection Officer is assigned and is not required. ○ The company is a public authority. ○ The company core activities require large scale, regular and systematic monitoring of individuals. ○ The company core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences. ○ The company is not required to appoint a DPO under the GDPR but has decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO and we support our DPO to the same standards.
companydpo.acct_dpo	no selection
companydpo.dpo_email	
companydpo.dpo_firstname	
companydpo.dpo_lastname	
companydpo.dpo_tel	
companydpo.dpo_mob	
companydpo.ico_reg	○ Yes ● No
companydpo.ico_number	

Please read through the criteria to decide if your business requires a DPO.

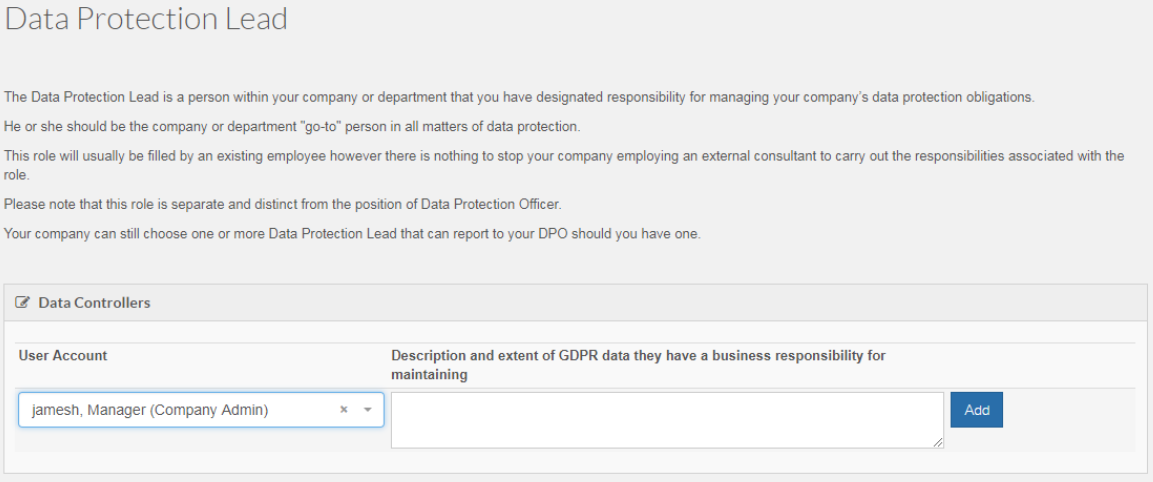
Once you have amended the details, please click the “Save” icon (Save) to save the information.

Please note that you will need to continue to add/remove any new/former DPOs as and when there is a change to ensure continued GPDR readiness.

Data Protection Lead(s)

The Data Protection lead is a person within your company or department that you have designated responsibility for managing your company's GDPR obligations.
He or she should be the company or department 'go-to' person in all matters of data protection.
This role will usually be filled by an existing employee however there is nothing to stop your company employing an external consultant to carry out the responsibilities associated with the role.
Please note that this role is separate and distinct from the position of Data Protection Officer.
Your company can still choose one or more Data Protection Leads that can report into your DPO should you have one.

Within this section you will need to select Data Protection Lead(s) from the drop down menu of Data Users. To determine who a Data Protection Lead is within your business, please refer to the "key responsibilities" information within the page.



Data Protection Lead

The Data Protection Lead is a person within your company or department that you have designated responsibility for managing your company's data protection obligations.

He or she should be the company or department "go-to" person in all matters of data protection.

This role will usually be filled by an existing employee however there is nothing to stop your company employing an external consultant to carry out the responsibilities associated with the role.

Please note that this role is separate and distinct from the position of Data Protection Officer.

Your company can still choose one or more Data Protection Lead that can report to your DPO should you have one.

Data Controllers

User Account	Description and extent of GDPR data they have a business responsibility for maintaining	
jamesh, Manager (Company Admin) × ▾		Add

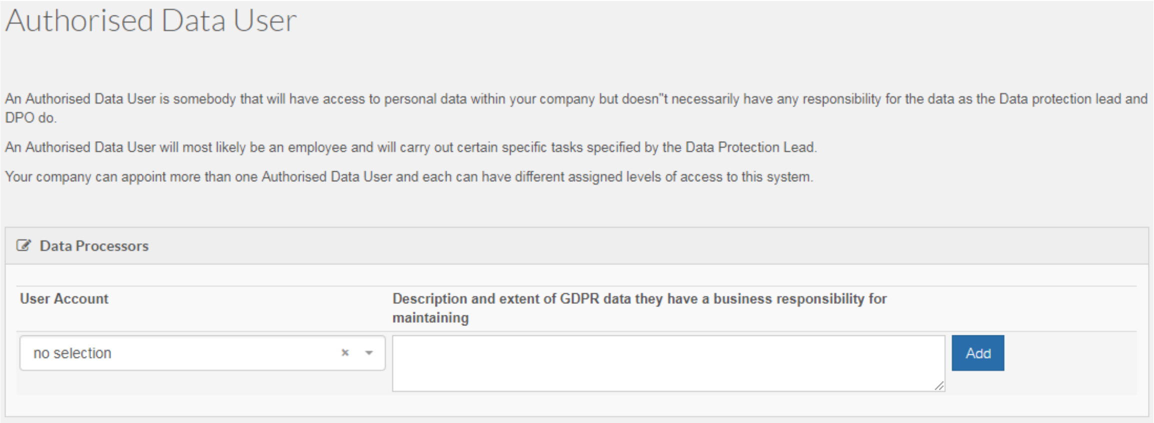
Once you have selected a Data Protection Lead, add a description of their data responsibilities and press "Add" (Add) to add to the list. You can select multiple Data Protection Leads.

Please note that you will need to continue to add/remove any new/former Data Protection Leads as and when there is a staff/responsibility change to ensure continued GPDR readiness.

Authorised Data User

An Authorised Data User is somebody that will have access to personal data within your company but doesn’t necessarily have any responsibility for the data as the Data Protection Lead and DPO do.
An Authorised Data User will most likely be an employee and will carry out certain specific tasks specified by the Data Protection Lead.
Your company can appoint more than one Authorised Data User and each can have different assigned levels of access to this system

Within this section you will need to select Authorised Data User(s) from the drop down menu of Data Users. To determine who an Authorised Data User is within your business, please refer to the “key responsibilities” information within the page.



Authorised Data User

An Authorised Data User is somebody that will have access to personal data within your company but doesn"t necessarily have any responsibility for the data as the Data protection lead and DPO do.

An Authorised Data User will most likely be an employee and will carry out certain specific tasks specified by the Data Protection Lead.

Your company can appoint more than one Authorised Data User and each can have different assigned levels of access to this system.

Data Processors

User Account	Description and extent of GDPR data they have a business responsibility for maintaining	
no selection × ▾		Add

Once you have selected an Authorised Data User, add a description of their data responsibilities and press “Add” (Add) to add to the list. You can select multiple Authorised Data Users.

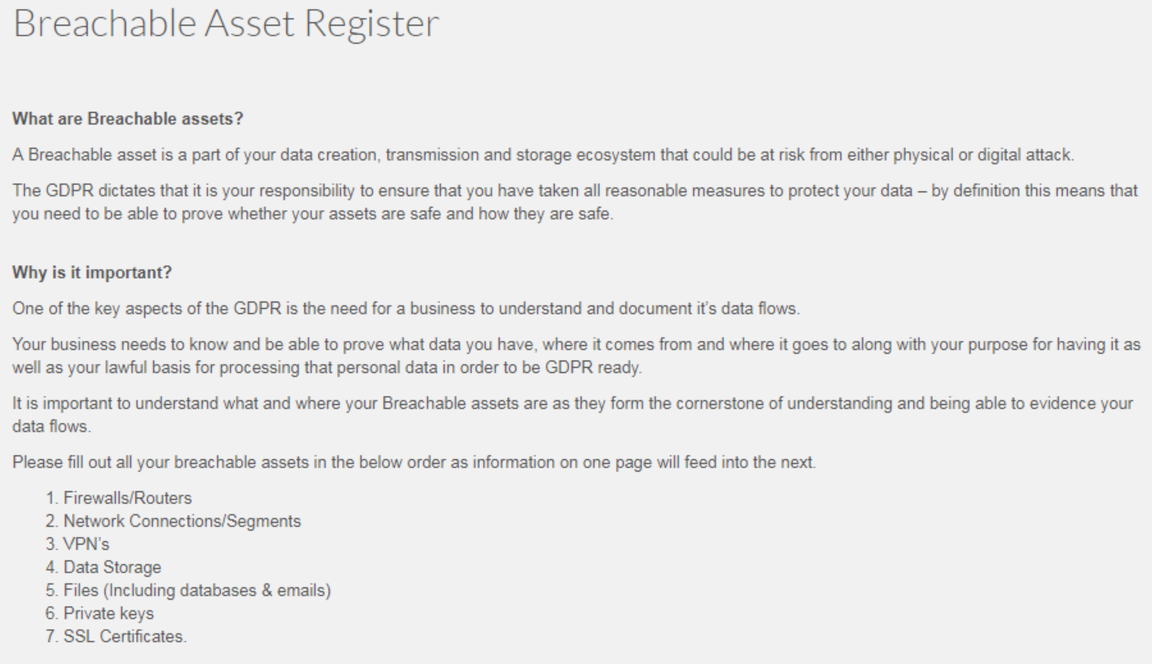
Please note that you will need to continue to add/remove any new/former Authorised Data Users as and when there is a change to ensure continued GPDR readiness.

Breachable Asset Register

A breachable asset is a part of your data creation, transmission and storage ecosystem that could be at risk from either physical or digital attack. These assets fall into seven categories:

1. Firewalls / Routers
2. Network Connections / Segments
3. VPNs
4. Storage Asset Information (Hardware)
5. Database and File Storage
6. Private Keys
7. SSL Certificates

Further explanation on the importance of this section can be found on this page.



Breachable Asset Register

What are Breachable assets?

A Breachable asset is a part of your data creation, transmission and storage ecosystem that could be at risk from either physical or digital attack.

The GDPR dictates that it is your responsibility to ensure that you have taken all reasonable measures to protect your data – by definition this means that you need to be able to prove whether your assets are safe and how they are safe.

Why is it important?

One of the key aspects of the GDPR is the need for a business to understand and document it's data flows.

Your business needs to know and be able to prove what data you have, where it comes from and where it goes to along with your purpose for having it as well as your lawful basis for processing that personal data in order to be GDPR ready.

It is important to understand what and where your Breachable assets are as they form the cornerstone of understanding and being able to evidence your data flows.

Please fill out all your breachable assets in the below order as information on one page will feed into the next.

1. Firewalls/Routers
2. Network Connections/Segments
3. VPN's
4. Data Storage
5. Files (Including databases & emails)
6. Private keys
7. SSL Certificates.

Firewalls / Routers

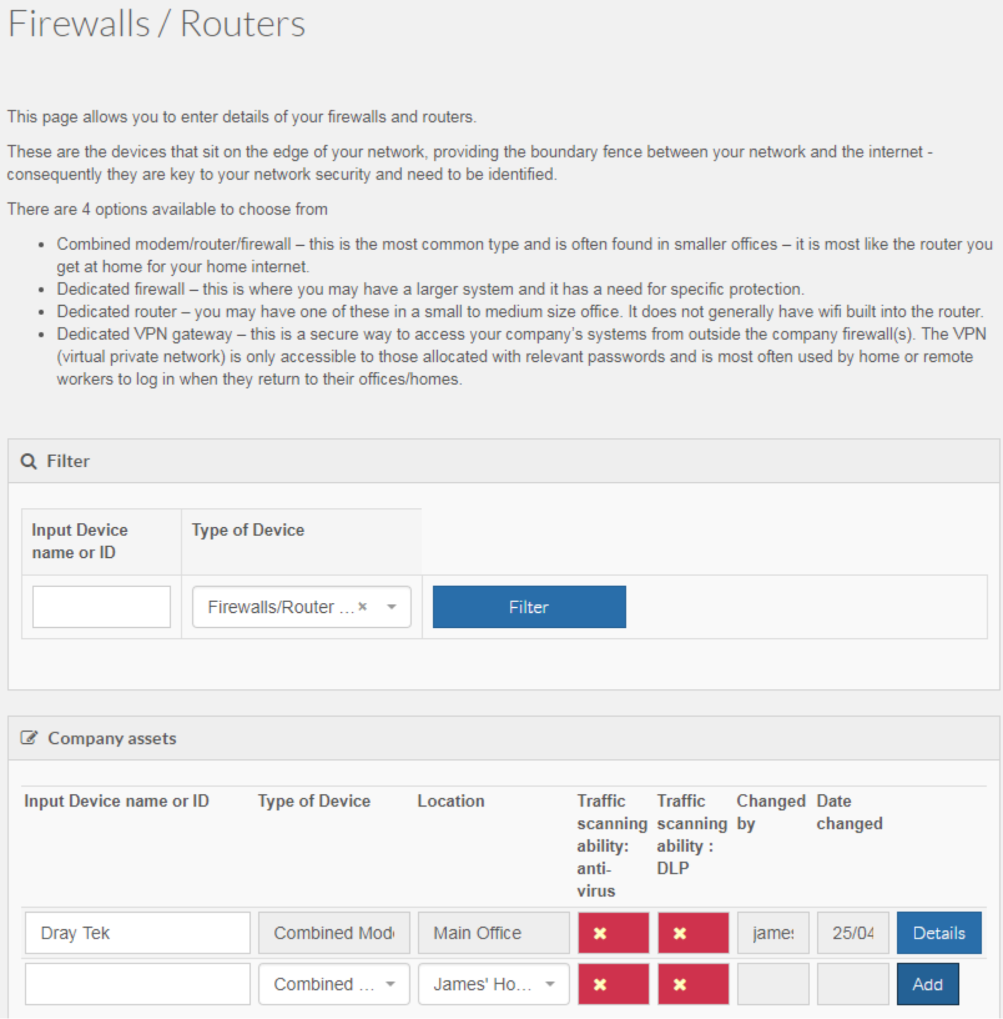
This page allows you to enter details of your firewalls and routers

These are the devices that provide a boundary fence between your network and the internet.

There are four options available to choose from:

1. Combined modem/router/firewall
2. Dedicated firewall
3. Dedicated router
4. Dedicated VPN gateway

At the top of this section is a search facility (Filter). This will come in handy once you have created a full list of personnel.



Firewalls / Routers

This page allows you to enter details of your firewalls and routers.

These are the devices that sit on the edge of your network, providing the boundary fence between your network and the internet - consequently they are key to your network security and need to be identified.

There are 4 options available to choose from

- Combined modem/router/firewall – this is the most common type and is often found in smaller offices – it is most like the router you get at home for your home internet.
- Dedicated firewall – this is where you may have a larger system and it has a need for specific protection.
- Dedicated router – you may have one of these in a small to medium size office. It does not generally have wifi built into the router.
- Dedicated VPN gateway – this is a secure way to access your company's systems from outside the company firewall(s). The VPN (virtual private network) is only accessible to those allocated with relevant passwords and is most often used by home or remote workers to log in when they return to their offices/homes.

Filter

Input Device name or ID	Type of Device	
	Firewalls/Router ... ×	Filter

Company assets

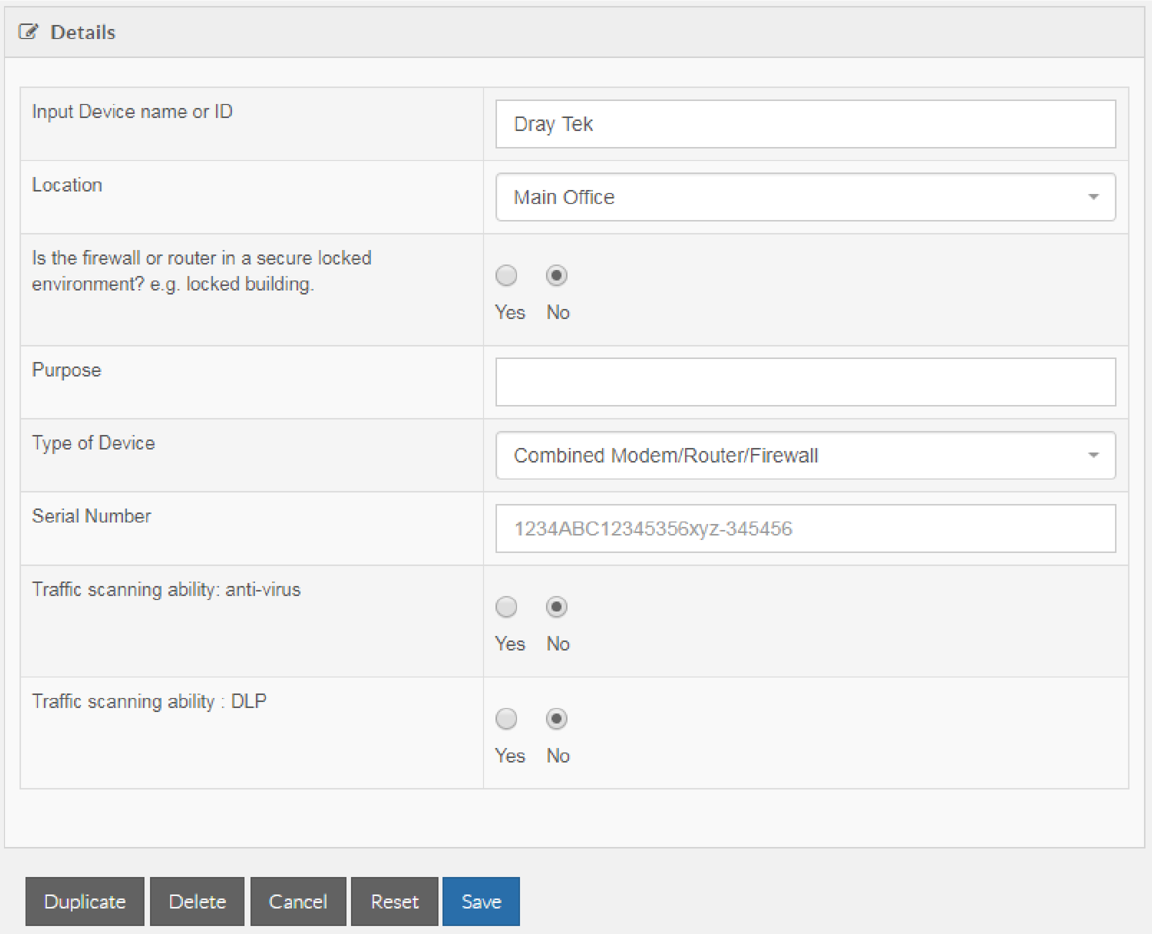
Input Device name or ID	Type of Device	Location	Traffic scanning ability: anti-virus	Traffic scanning ability : DLP	Changed by	Date changed	
Dray Tek	Combined Mod	Main Office	✖	✖	jame:	25/04	Details
	Combined ...	James' Ho...	✖	✖			Add

Below the search facility is a list of the devices you will have added. At the bottom of the screen you are able to add (further) devices.

To add an entry, give the devise a unique name, select the type of device and its location from the drop-down menus provided and click “Add” (Add).

Once added, you can click on the “Details” (Details) button to add further information about the device, including serial numbers and the purpose of the device.

From here you will be able to answer questions about whether the device has traffic scanning ability (anti-virus or Data Loss Prevention (DLP). When answered it show you the red cross (✖) or a green tick (✓) to demonstrate how secure the device is.



Details

Input Device name or ID	Dray Tek
Location	Main Office
Is the firewall or router in a secure locked environment? e.g. locked building.	○ Yes ● No
Purpose	
Type of Device	Combined Modem/Router/Firewall
Serial Number	1234ABC12345356xyz-345456
Traffic scanning ability: anti-virus	○ Yes ● No
Traffic scanning ability : DLP	○ Yes ● No

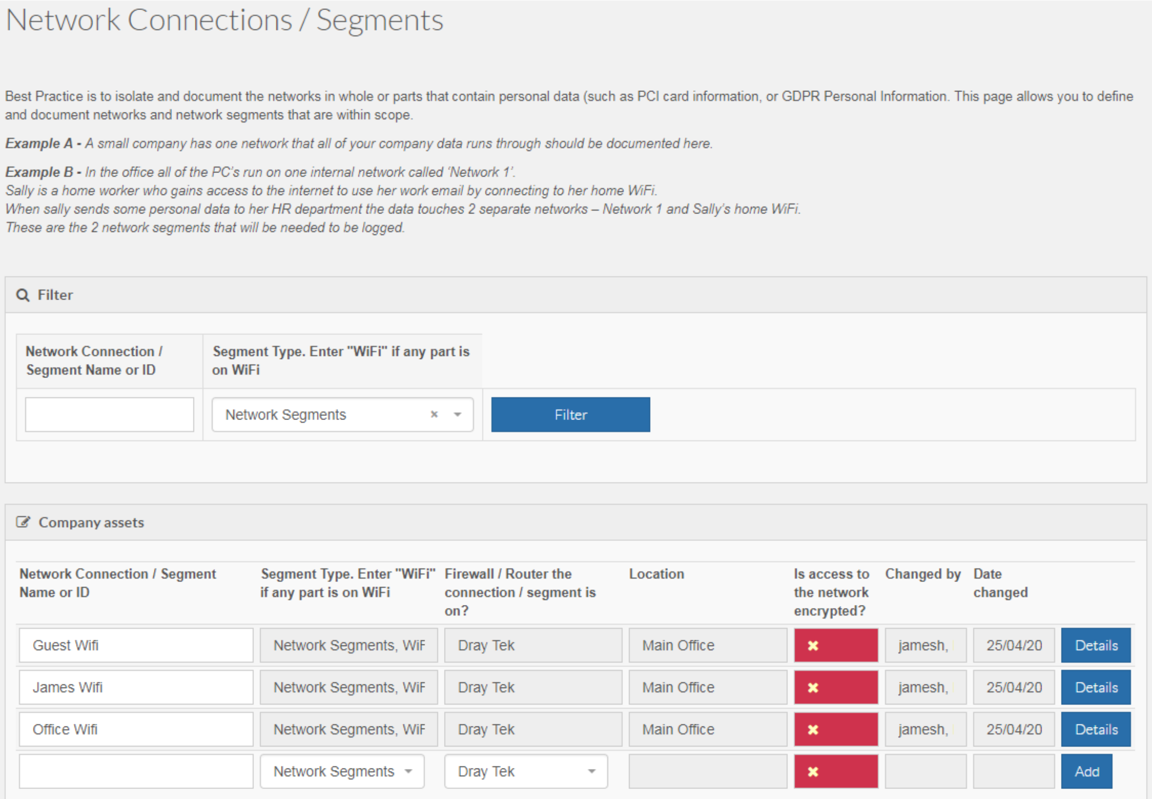
Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

Network Connections / Segments

This page allows you to define and document networks and network segments. Examples of this are detailed on the page.

You will need to list all network connections, including staff's home connections, if they access work information from their personal Wi-Fi / broadband.

At the top of this section is a search facility (Filter). This will come in handy once you have created a full list of devices.



Network Connections / Segments

Best Practice is to isolate and document the networks in whole or parts that contain personal data (such as PCI card information, or GDPR Personal Information. This page allows you to define and document networks and network segments that are within scope.

Example A - *A small company has one network that all of your company data runs through should be documented here.*

Example B - *In the office all of the PC's run on one internal network called 'Network 1'.*
Sally is a home worker who gains access to the internet to use her work email by connecting to her home WiFi.
When sally sends some personal data to her HR department the data touches 2 separate networks – Network 1 and Sally's home WiFi.
These are the 2 network segments that will be needed to be logged.

Filter

Network Connection / Segment Name or ID	Segment Type. Enter "WiFi" if any part is on WiFi	
	Network Segments	Filter

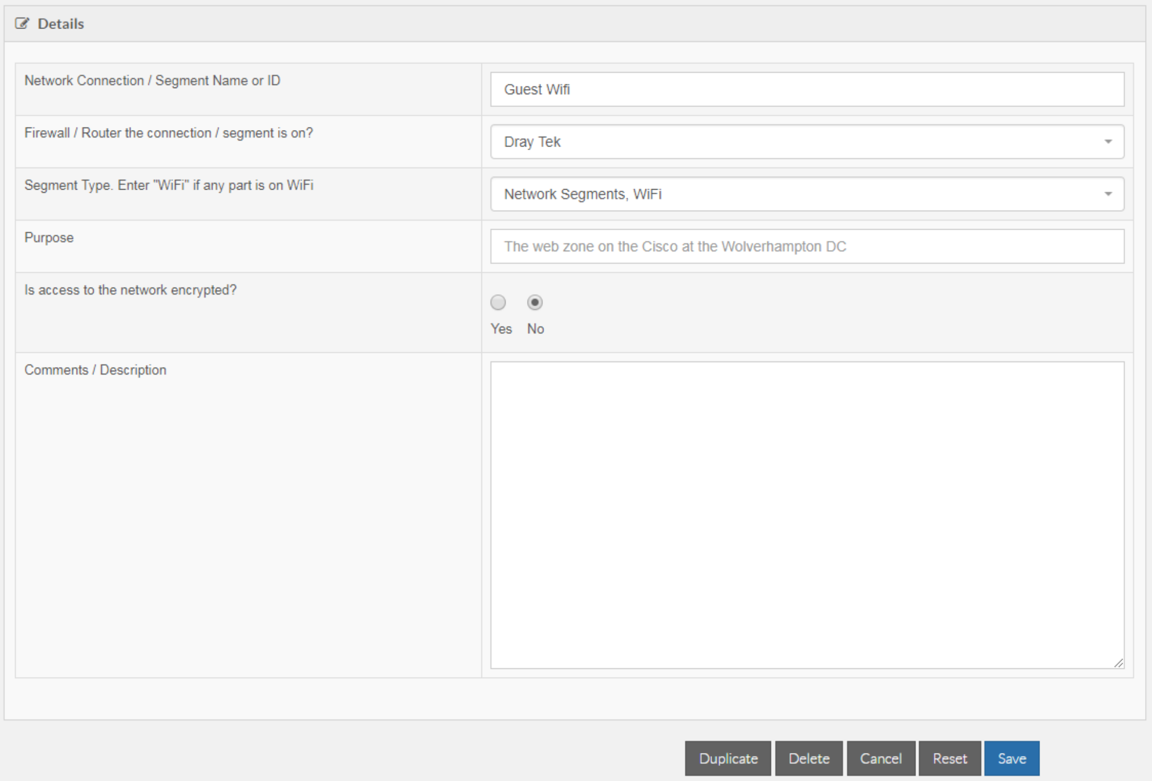
Company assets

Network Connection / Segment Name or ID	Segment Type. Enter "WiFi" if any part is on WiFi	Firewall / Router the connection / segment is on?	Location	Is access to the network encrypted?	Changed by	Date changed	
Guest Wifi	Network Segments, WiF	Dray Tek	Main Office	✖	jamesh,	25/04/20	Details
James Wifi	Network Segments, WiF	Dray Tek	Main Office	✖	jamesh,	25/04/20	Details
Office Wifi	Network Segments, WiF	Dray Tek	Main Office	✖	jamesh,	25/04/20	Details
	Network Segments	Dray Tek		✖			Add

Below the search facility is a list of the connections you will have added. At the bottom of the screen you are able to add (further) connections.

To add an entry, give the connection a unique name, select the segment type, which device it uses and its location from the drop-down menus provided and click "Add" (Add). From here you can also see if the access to the network is encrypted.

Once added, you can click on the "Details" (Details) button to add further information about the network connection(s) and to turn the dashboard from a red cross to a green tick you will need to input details of how the device(s) are safe.



Details

Network Connection / Segment Name or ID	Guest Wifi
Firewall / Router the connection / segment is on?	Dray Tek
Segment Type. Enter "WiFi" if any part is on WiFi	Network Segments, WiFi
Purpose	The web zone on the Cisco at the Wolverhampton DC
Is access to the network encrypted?	○ Yes ● No
Comments / Description	

Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

VPNs

A Virtual Private Network (VPN) will normally either be connections to a partner organisation or a means for company users to access data remotely via the internet.

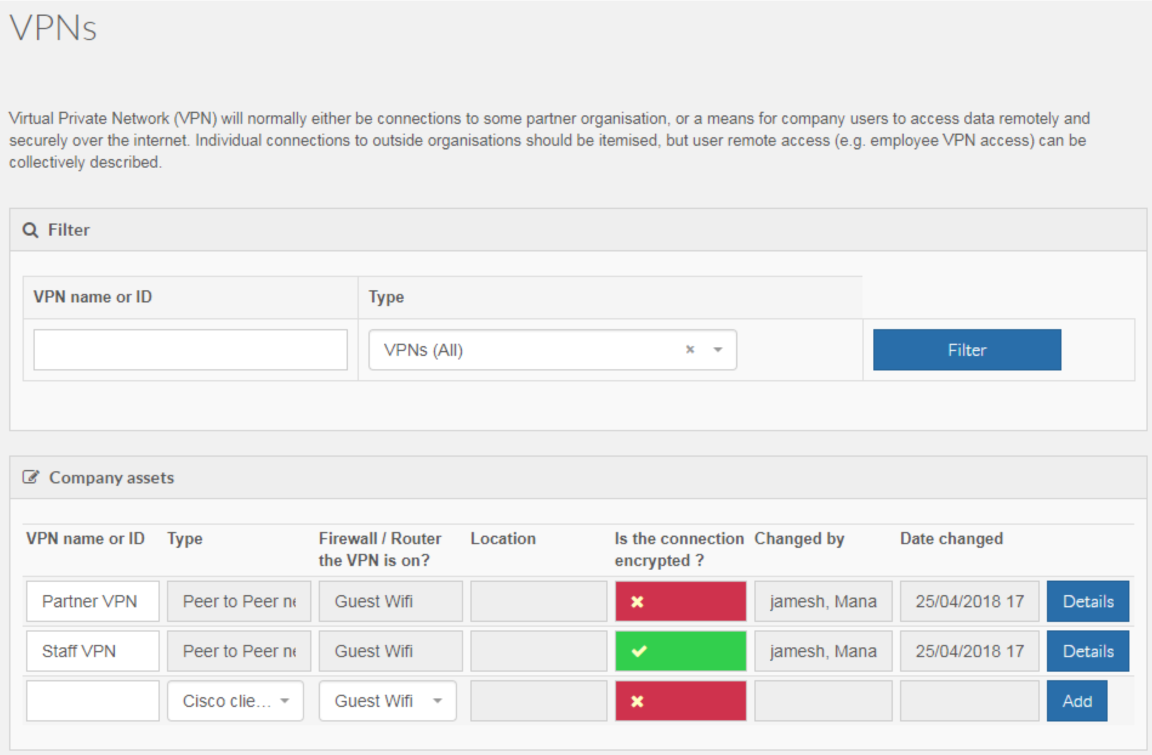
Individual connections to outside organisations should be itemised but user remote access (staff remotely logging in) can be collectively described.

There are three main types of VPN:

1. Cisco client VPN
2. Peer to Peer VPN
3. SSL client VPN

You will need to select one of these for each VPN listed. For further information, please consult with your IT provider.

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of VPNs.



VPNs

Virtual Private Network (VPN) will normally either be connections to some partner organisation, or a means for company users to access data remotely and securely over the internet. Individual connections to outside organisations should be itemised, but user remote access (e.g. employee VPN access) can be collectively described.

Filter

VPN name or ID	Type	
	VPNs (All) ×	Filter

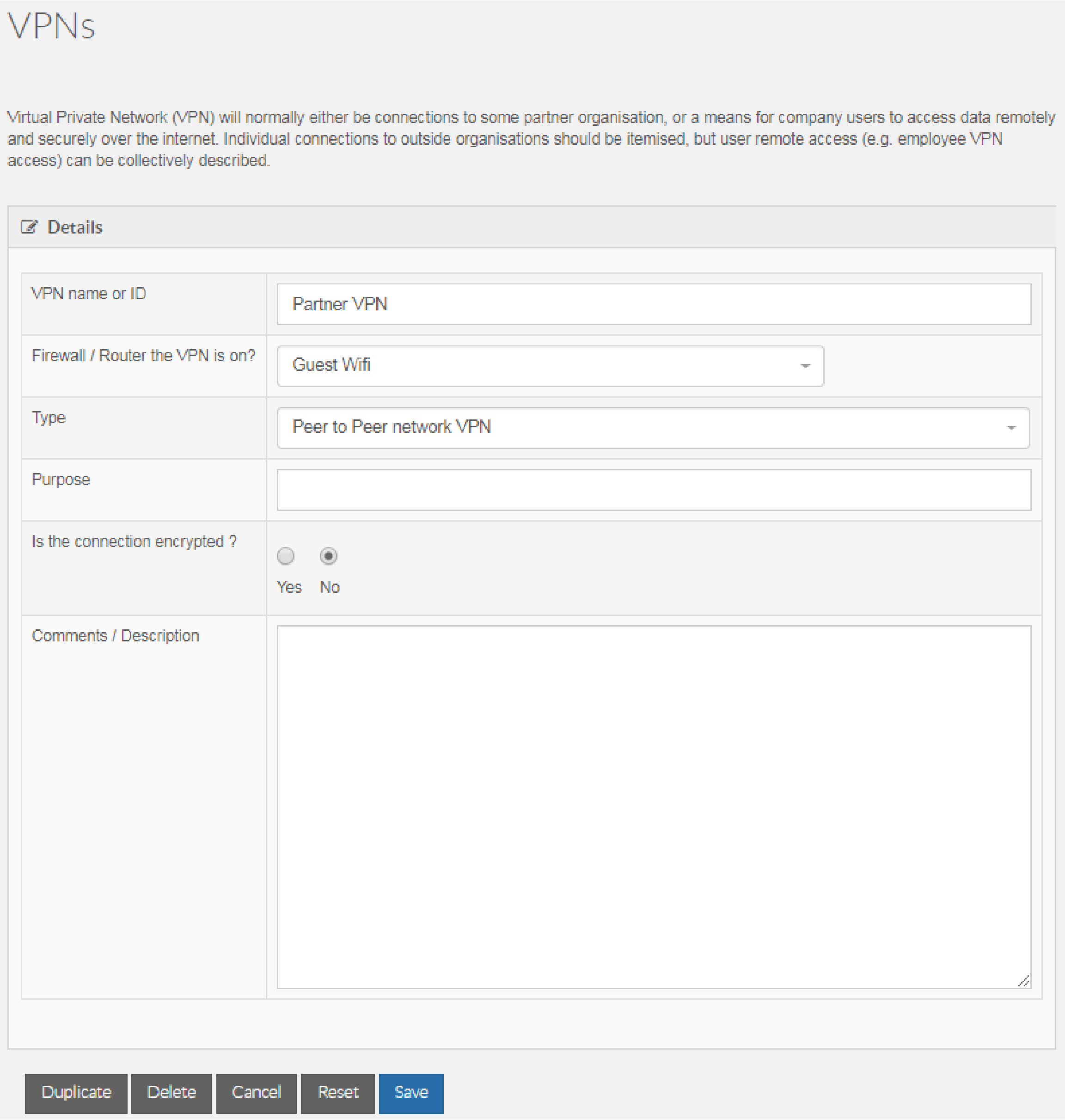
Company assets

VPN name or ID	Type	Firewall / Router the VPN is on?	Location	Is the connection encrypted ?	Changed by	Date changed	
Partner VPN	Peer to Peer n	Guest Wifi		✗	jamesh, Mana	25/04/2018 17	Details
Staff VPN	Peer to Peer n	Guest Wifi		✓	jamesh, Mana	25/04/2018 17	Details
	Cisco clie…	Guest Wifi		✗			Add

Below the search facility is a list of the VPNs you will have added. At the bottom of the screen you are able to add (further) VPNs.

To add an entry, give the VPN a unique name, select the type, which device it uses and its location from the drop-down menus provided and click “Add” (Add). From here you can also see if the connection is encrypted.

Once added, you can click on the “Details” (Details) button to add further information about the VPN and evidence how it is encrypted.



VPNs

Virtual Private Network (VPN) will normally either be connections to some partner organisation, or a means for company users to access data remotely and securely over the internet. Individual connections to outside organisations should be itemised, but user remote access (e.g. employee VPN access) can be collectively described.

Details

VPN name or ID	Partner VPN
Firewall / Router the VPN is on?	Guest Wifi
Type	Peer to Peer network VPN
Purpose	
Is the connection encrypted ?	○ Yes ● No
Comments / Description	

Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

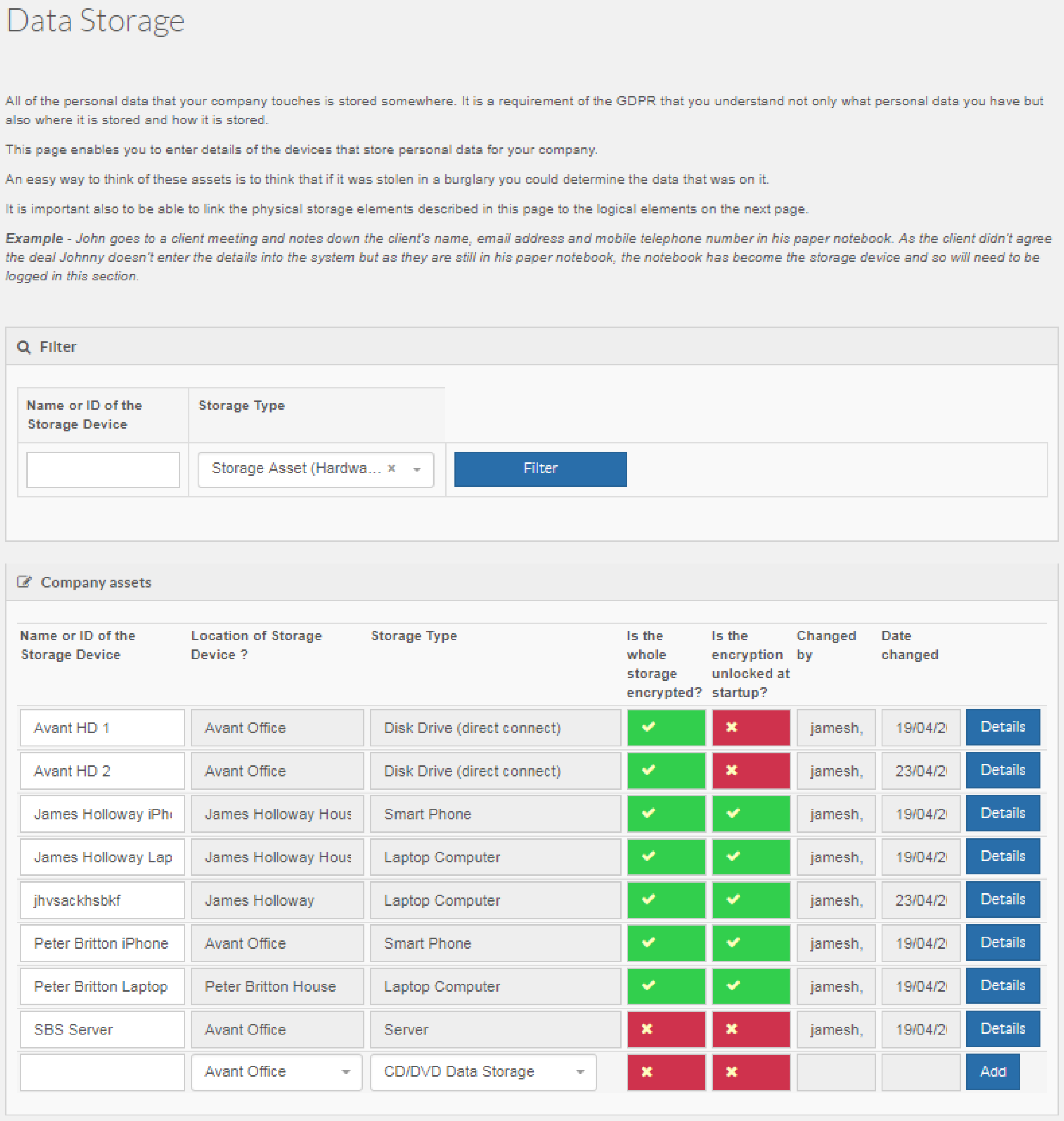
Storage Asset Information (Hardware)

This page enables you to enter details of the devices that store personal data for your company.
Please note that this is not limited to electronical devices; you may have paper based personal details stored in e.g. a filing cabinet. These would also have to be listed as a data storage asset.

Types of devices include (but are not limited to):

- CD/DVD Data Storage
- Cloud (Private)
- Cloud (Public / External)
- Desk Draws (Lockable)
- Desktop Computer
- Disk Drive
- Laptop Computer
- Lockable Filing Cabinet
- Memory Sticks
- Network Storage
- Note Books (paper)
- Safe
- Server
- Smart Phone
- Tablet
- Website

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of storage devices.



Data Storage

All of the personal data that your company touches is stored somewhere. It is a requirement of the GDPR that you understand not only what personal data you have but also where it is stored and how it is stored.

This page enables you to enter details of the devices that store personal data for your company.

An easy way to think of these assets is to think that if it was stolen in a burglary you could determine the data that was on it.

It is important also to be able to link the physical storage elements described in this page to the logical elements on the next page.

***Example** - John goes to a client meeting and notes down the client's name, email address and mobile telephone number in his paper notebook. As the client didn't agree the deal Johnny doesn't enter the details into the system but as they are still in his paper notebook, the notebook has become the storage device and so will need to be logged in this section.*

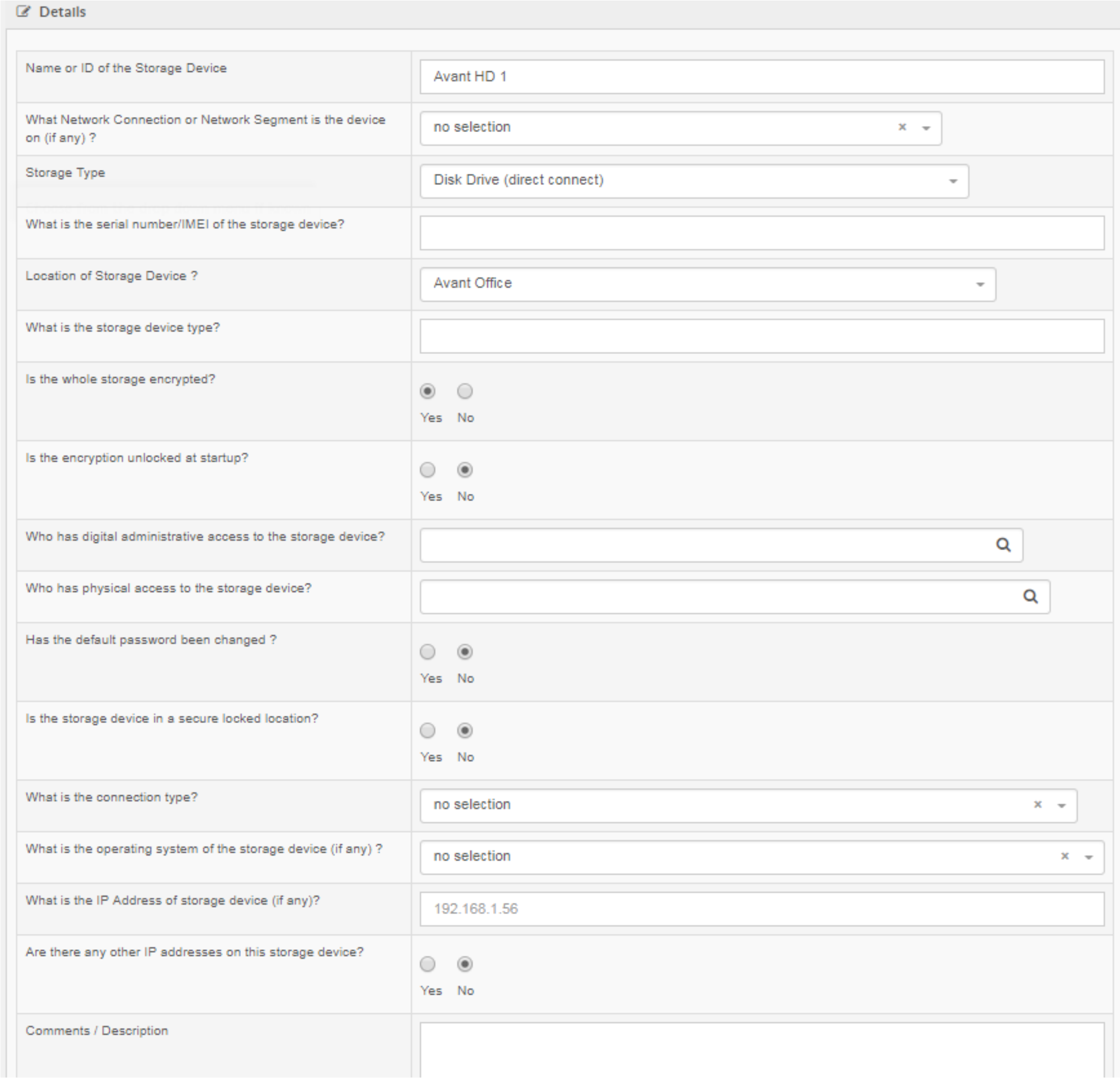
Name or ID of the Storage Device	Storage Type	
	Storage Asset (Hardwa… ×	Filter

Name or ID of the Storage Device	Location of Storage Device ?	Storage Type	Is the whole storage encrypted?	Is the encryption unlocked at startup?	Changed by	Date changed	
Avant HD 1	Avant Office	Disk Drive (direct connect)	✓	✖	jamesh,	19/04/2	Details
Avant HD 2	Avant Office	Disk Drive (direct connect)	✓	✖	jamesh,	23/04/2	Details
James Holloway iPh	James Holloway Hous	Smart Phone	✓	✓	jamesh,	19/04/2	Details
James Holloway Lap	James Holloway Hous	Laptop Computer	✓	✓	jamesh,	19/04/2	Details
jhvsackhsbkf	James Holloway	Laptop Computer	✓	✓	jamesh,	23/04/2	Details
Peter Britton iPhone	Avant Office	Smart Phone	✓	✓	jamesh,	19/04/2	Details
Peter Britton Laptop	Peter Britton House	Laptop Computer	✓	✓	jamesh,	19/04/2	Details
SBS Server	Avant Office	Server	✖	✖	jamesh,	19/04/2	Details
	Avant Office	CD/DVD Data Storage	✖	✖			Add

Below the search facility is a list of the devises you will have added. At the bottom of the screen you are able to add (further) devises.

To add an entry, give the device a unique name, then select the location and storage type from the drop down menus provided and click "Add" (Add). From here you can also see if the device is encrypted.

Once added, you can click on the "Details" (Details) button to add further information about the device, including serial number, IP address and who has access to the device as well as what type of encryption is used.



Details

Name or ID of the Storage Device	Avant HD 1
What Network Connection or Network Segment is the device on (if any) ?	no selection ×
Storage Type	Disk Drive (direct connect)
What is the serial number/IMEI of the storage device?	
Location of Storage Device ?	Avant Office
What is the storage device type?	
Is the whole storage encrypted?	● Yes ○ No
Is the encryption unlocked at startup?	○ Yes ● No
Who has digital administrative access to the storage device?	
Who has physical access to the storage device?	
Has the default password been changed ?	○ Yes ● No
Is the storage device in a secure locked location?	○ Yes ● No
What is the connection type?	no selection ×
What is the operating system of the storage device (if any) ?	no selection ×
What is the IP Address of storage device (if any)?	192.168.1.56
Are there any other IP addresses on this storage device?	○ Yes ● No
Comments / Description	

Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

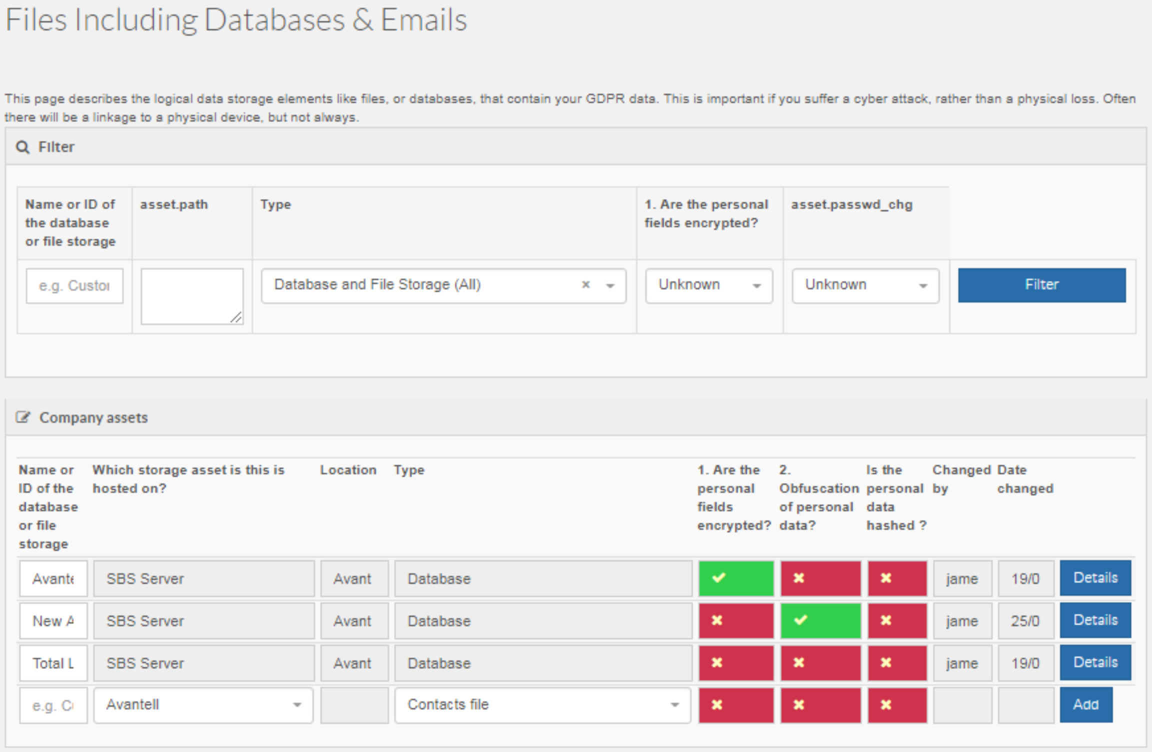
Database and File Storage

In this section you will list your file storage, including databases and email.

Types of file storage include:

- Contacts File
- Database
- Email
- Mail merge source files
- Other text files
- Spreadsheets
- Word documents

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of storage devises.



Files Including Databases & Emails

This page describes the logical data storage elements like files, or databases, that contain your GDPR data. This is important if you suffer a cyber attack, rather than a physical loss. Often there will be a linkage to a physical device, but not always.

Filter

Name or ID of the database or file storage	asset.path	Type	1. Are the personal fields encrypted?	asset.passwd_chg	
e.g. Custo		Database and File Storage (All)	Unknown	Unknown	Filter

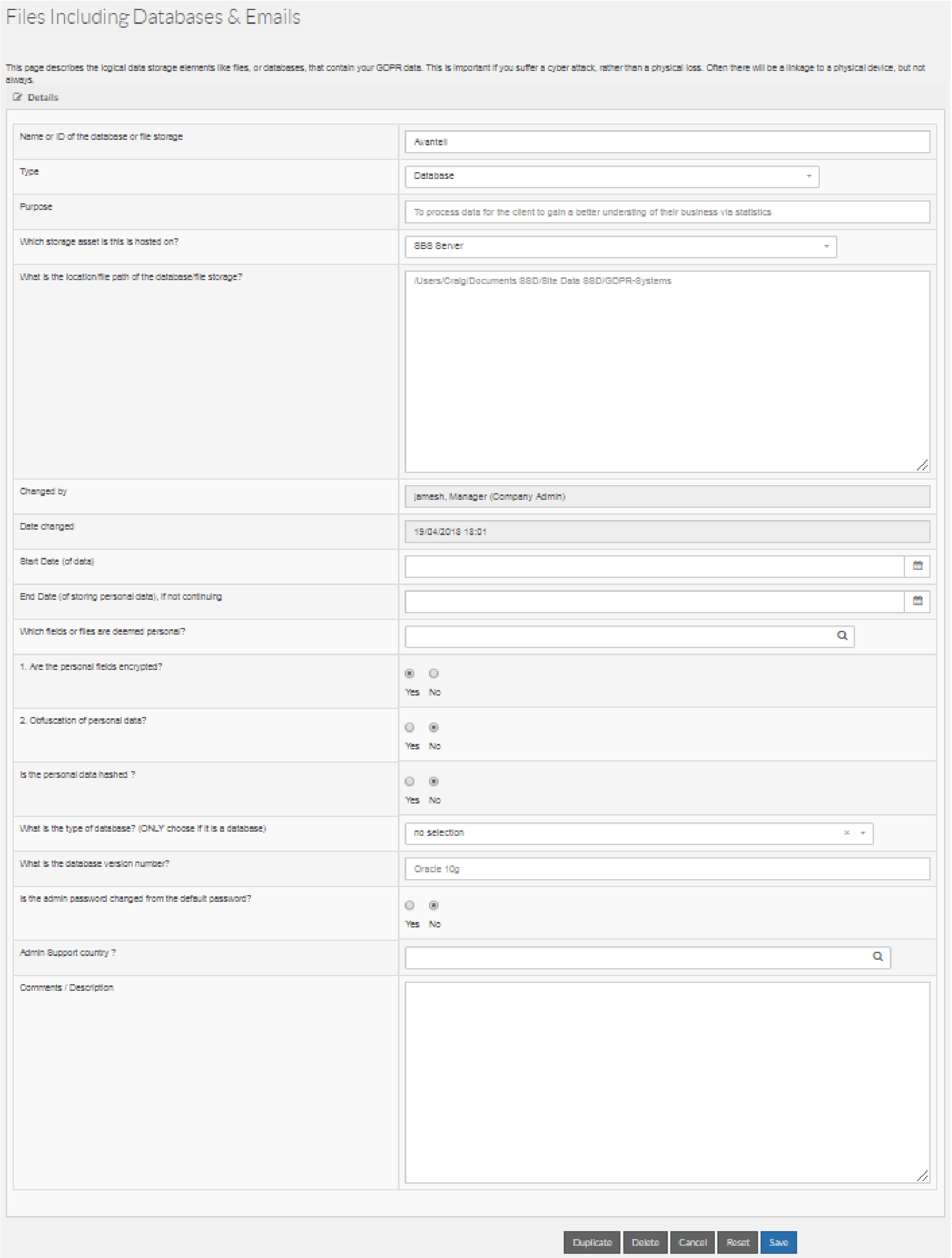
Company assets

Name or ID of the database or file storage	Which storage asset is this is hosted on?	Location	Type	1. Are the personal fields encrypted?	2. Obfuscation of personal data?	Is the personal data hashed ?	Changed by	Date changed	
Avante	SBS Server	Avant	Database	✓	✗	✗	jame	19/0	Details
New A	SBS Server	Avant	Database	✗	✓	✗	jame	25/0	Details
Total L	SBS Server	Avant	Database	✗	✗	✗	jame	19/0	Details
e.g. C	Avantell		Contacts file	✗	✗	✗			Add

Below the search facility is a list of the file storage you will have added. At the bottom of the screen you are able to add (further) file storage.

To add an entry, give the file storage a unique name, then state which storage asset it is hosted on, its location and type from the drop-down menus provided and click "Add" (Add). From here you can also see if the personal fields are encrypted or if they are obfuscated (blanked out) or hashed (typed over with e.g. an "*").

Once added, you can click on the "Details" (Details) button to add further information about the file storage, including which fields are deemed private.



Files Including Databases & Emails

This page describes the logical data storage elements like files, or databases, that contain your GDPR data. This is important if you suffer a cyber attack, rather than a physical loss. Often there will be a linkage to a physical device, but not always.

Details

Name or ID of the database or file storage	Avantell
Type	Database
Purpose	To process data for the client to gain a better understing of their business via statistics
Which storage asset is this is hosted on?	SBS Server
What is the location/file path of the database/file storage?	/Users/Craig/Documents SSD/Site Data SSD/GDPR-Systems
Changed by	jamesh, Manager (Company Admin)
Date changed	19/04/2018 18:01
Start Date (of data)	
End Date (of storing personal data), if not continuing	
Which fields or files are deemed personal?	
1. Are the personal fields encrypted?	● Yes ○ No
2. Obfuscation of personal data?	○ Yes ● No
Is the personal data hashed ?	○ Yes ● No
What is the type of database? (ONLY choose if it is a database)	no selection
What is the database version number?	Oracle 10g
Is the admin password changed from the default password?	○ Yes ● No
Admin Support country ?	
Comments / Description	

Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

Private Keys

Public Key Infrastructure (PKI) comes in two parts; the public key (shared with whomever you are communicating) and the private key part. It is critical that the private key is kept safe – not only does it encrypt your data, but it can be used to authenticate (i.e. impersonate) you to others.

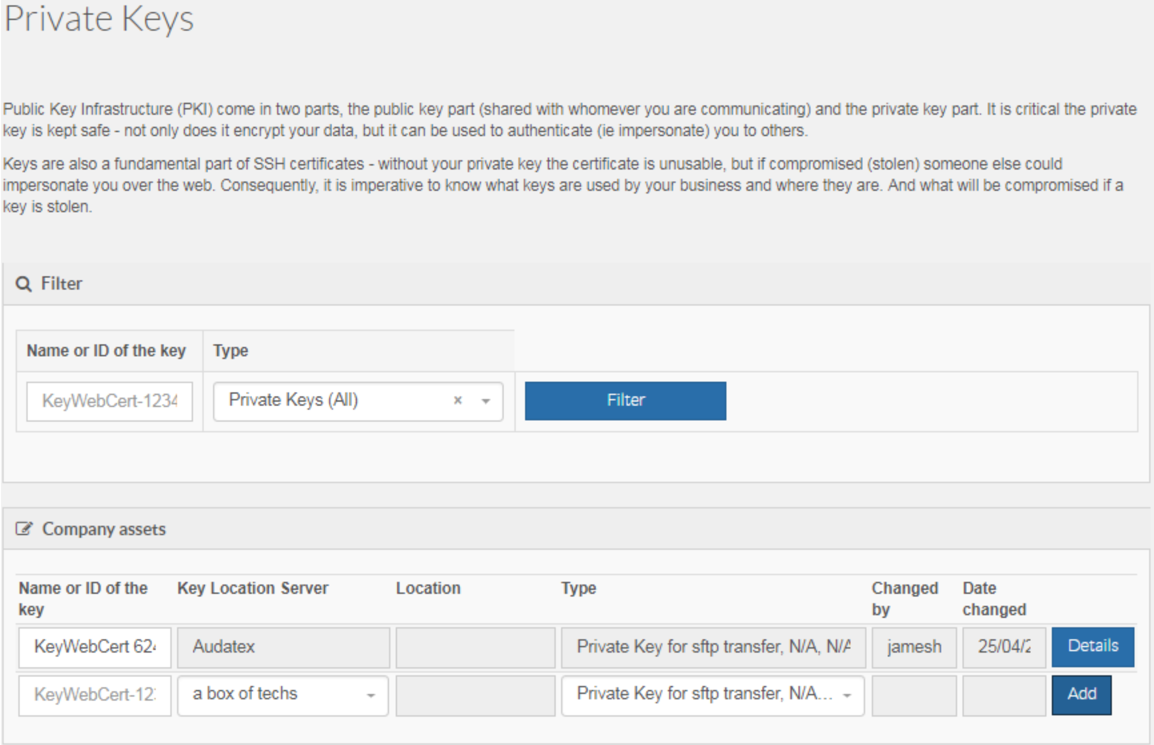
For further information regarding private keys, please consult with your IT provider.

In this section you will list your file storage, including databases and email.

There are three types of private key:

1. Private key for sttp transfer
2. Private key for SSL certificate
3. Private PGP key

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of private keys.



Private Keys

Public Key Infrastructure (PKI) come in two parts, the public key part (shared with whomever you are communicating) and the private key part. It is critical the private key is kept safe - not only does it encrypt your data, but it can be used to authenticate (ie impersonate) you to others.

Keys are also a fundamental part of SSH certificates - without your private key the certificate is unusable, but if compromised (stolen) someone else could impersonate you over the web. Consequently, it is imperative to know what keys are used by your business and where they are. And what will be compromised if a key is stolen.

Filter

Name or ID of the key	Type	
KeyWebCert-1234	Private Keys (All) ×	Filter

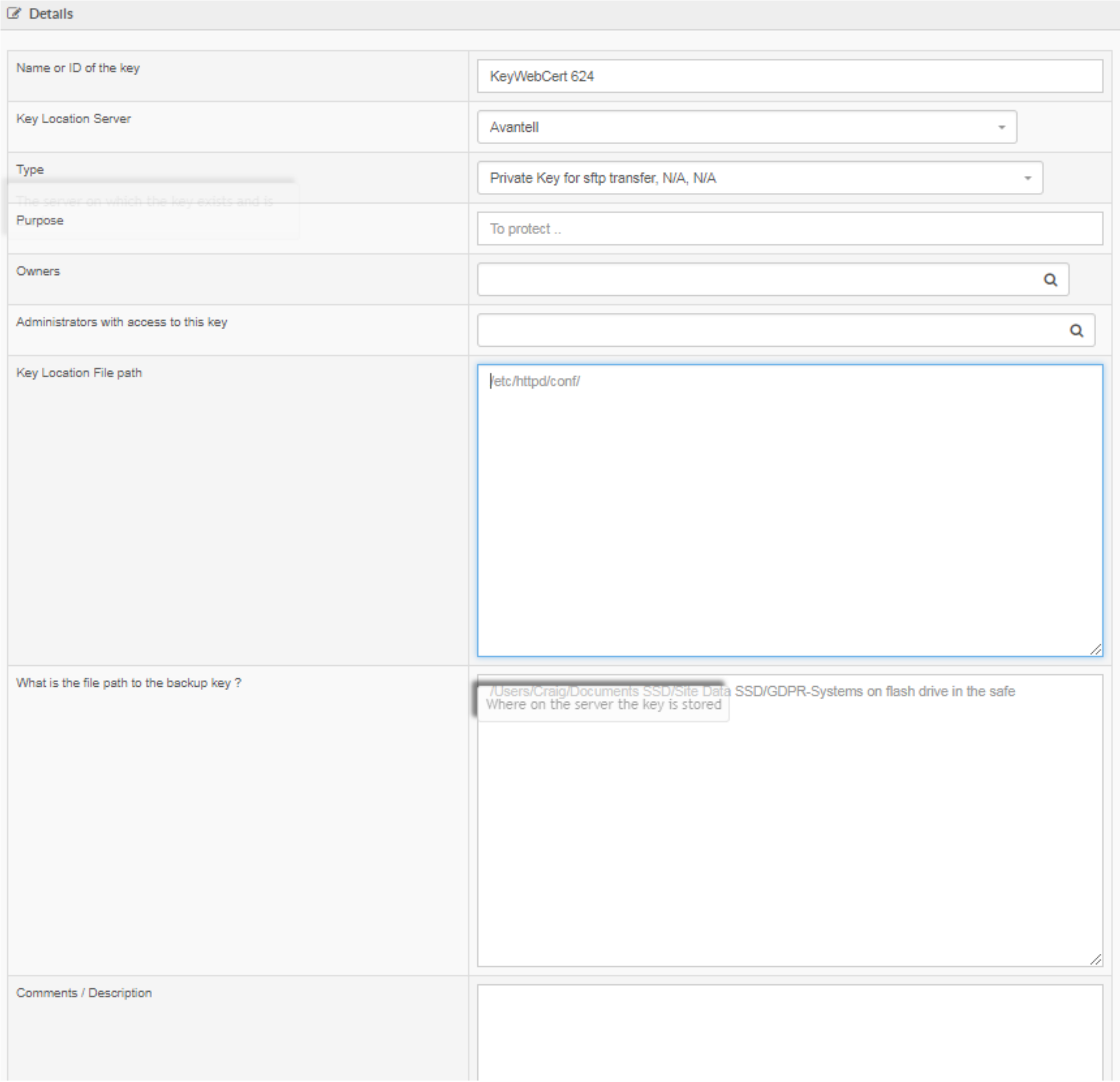
Company assets

Name or ID of the key	Key Location Server	Location	Type	Changed by	Date changed	
KeyWebCert 62	Audatex		Private Key for sftp transfer, N/A, N/A	jamesh	25/04/2	Details
KeyWebCert-12	a box of techs		Private Key for sftp transfer, N/A...			Add

Below the search facility is a list of the private keys you will have added. At the bottom of the screen you are able to add (further) private keys.

To add an entry, give the private key a unique name, then state which location server is used and what type of key it is from the drop-down menus provided and click “Add” (Add).

Once added, you can click on the “Details” (Details) button to add further information about the file storage, including the owner, key location file path and backup details.



Details

Name or ID of the key	KeyWebCert 624
Key Location Server	Avantell
Type	Private Key for sftp transfer, N/A, N/A
Purpose	To protect ..
Owners	
Administrators with access to this key	
Key Location File path	/etc/httpd/conf/
What is the file path to the backup key ?	/Users/Craig/Documents SSD/Site Data SSD/GDPR-Systems on flash drive in the safe
Comments / Description	

The server on which the key exists and is
Where on the server the key is stored

Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

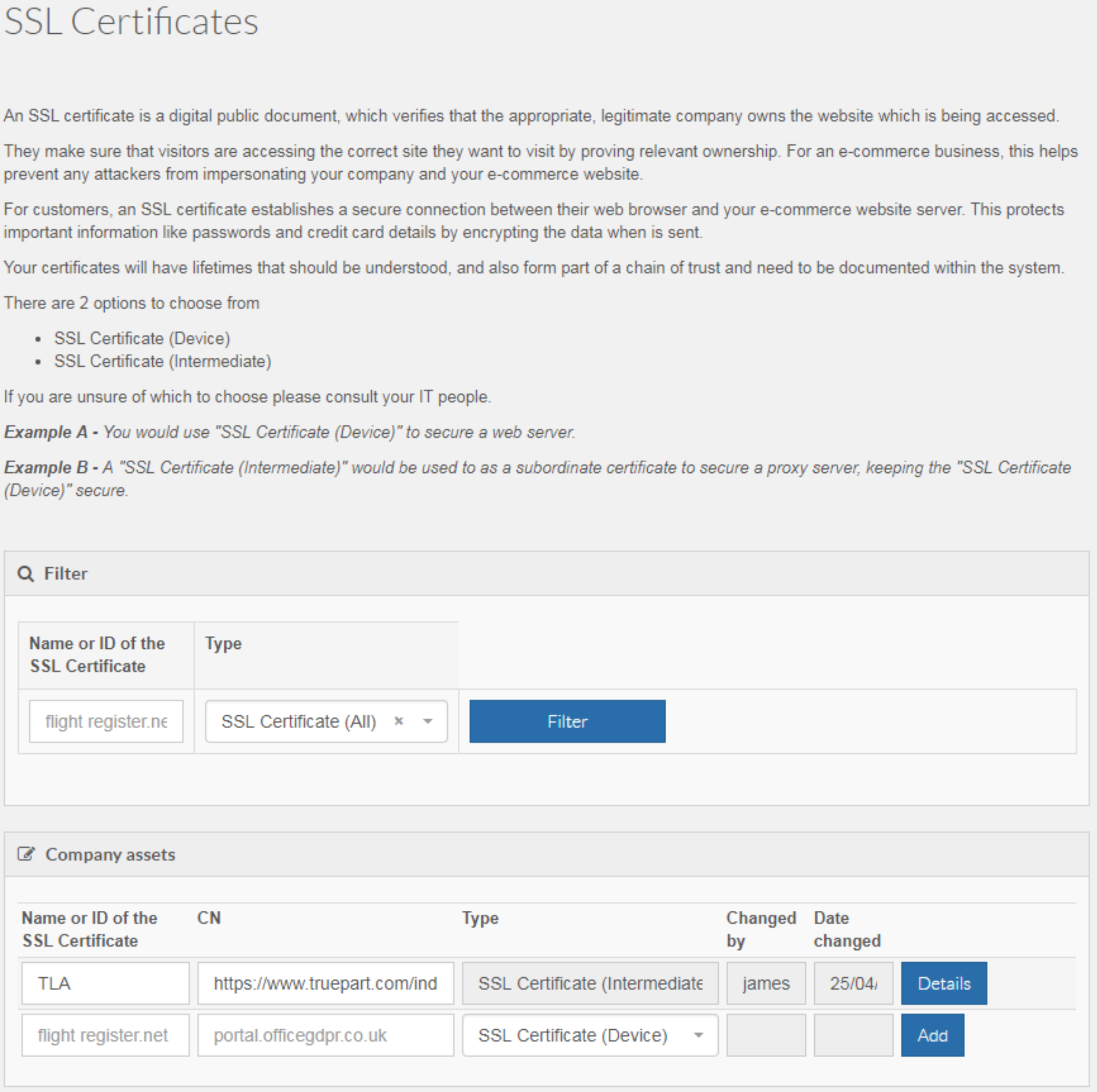
SSL Certificates

An SSL certificate is a digital public document which verifies that the appropriate, legitimate company owns the website that is being accessed.

They make sure that the visitors are accessing the correct site they intended to visit by providing relevant ownership – this helps prevent any attackers from impersonating your company and website.

For customers, an SSL certificate establishes a secure connection between their web browser and your website server. This protects important information like passwords by encrypting the data when it is sent.

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of private keys.



SSL Certificates

An SSL certificate is a digital public document, which verifies that the appropriate, legitimate company owns the website which is being accessed.

They make sure that visitors are accessing the correct site they want to visit by proving relevant ownership. For an e-commerce business, this helps prevent any attackers from impersonating your company and your e-commerce website.

For customers, an SSL certificate establishes a secure connection between their web browser and your e-commerce website server. This protects important information like passwords and credit card details by encrypting the data when is sent.

Your certificates will have lifetimes that should be understood, and also form part of a chain of trust and need to be documented within the system.

There are 2 options to choose from

- SSL Certificate (Device)
- SSL Certificate (Intermediate)

If you are unsure of which to choose please consult your IT people.

Example A - *You would use "SSL Certificate (Device)" to secure a web server.*

Example B - *A "SSL Certificate (Intermediate)" would be used to as a subordinate certificate to secure a proxy server, keeping the "SSL Certificate (Device)" secure.*

Filter

Name or ID of the SSL Certificate	Type	
flight register.ne	SSL Certificate (All) ×	Filter

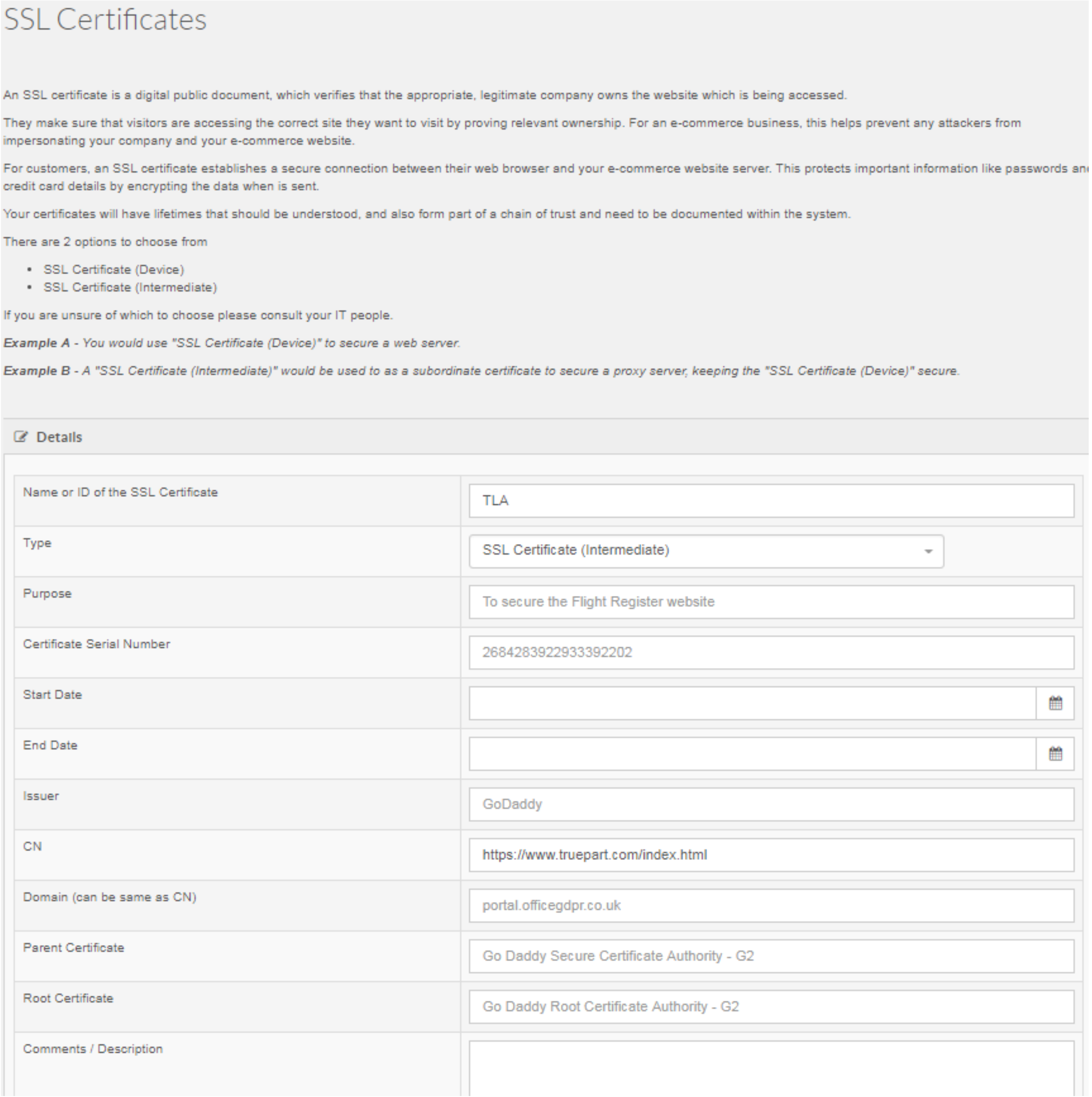
Company assets

Name or ID of the SSL Certificate	CN	Type	Changed by	Date changed	
TLA	https://www.truepart.com/ind	SSL Certificate (Intermediate	james	25/04/	Details
flight register.net	portal.officegdpr.co.uk	SSL Certificate (Device)			Add

Below the search facility is a list of the SSL certificates you will have added. At the bottom of the screen you are able to add (further) SSL certificates.

To add an entry, give the SSL certificate a unique name, then state which storage asset it is hosted on, its location and type from the drop-down menus provided and click “Add” (Add).

Once added, you can click on the “Details” (Details) button to add further information about the file storage, including domain name and other certificate details.



SSL Certificates

An SSL certificate is a digital public document, which verifies that the appropriate, legitimate company owns the website which is being accessed.

They make sure that visitors are accessing the correct site they want to visit by proving relevant ownership. For an e-commerce business, this helps prevent any attackers from impersonating your company and your e-commerce website.

For customers, an SSL certificate establishes a secure connection between their web browser and your e-commerce website server. This protects important information like passwords an credit card details by encrypting the data when is sent.

Your certificates will have lifetimes that should be understood, and also form part of a chain of trust and need to be documented within the system.

There are 2 options to choose from

- SSL Certificate (Device)
- SSL Certificate (Intermediate)

If you are unsure of which to choose please consult your IT people.

Example A *- You would use "SSL Certificate (Device)" to secure a web server.*

Example B *- A "SSL Certificate (Intermediate)" would be used to as a subordinate certificate to secure a proxy server, keeping the "SSL Certificate (Device)" secure.*

Details

Name or ID of the SSL Certificate	TLA
Type	SSL Certificate (Intermediate)
Purpose	To secure the Flight Register website
Certificate Serial Number	2684283922933392202
Start Date	
End Date	
Issuer	GoDaddy
CN	https://www.truepart.com/index.html
Domain (can be same as CN)	portal.officegdpr.co.uk
Parent Certificate	Go Daddy Secure Certificate Authority - G2
Root Certificate	Go Daddy Root Certificate Authority - G2
Comments / Description	

Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

Data Transfers

It is important that you document how data moves around your business. This may be data you receive, data you send or data the moves internally within the business.

You must be able to detail why you have the information, the methods used for transferring data and the security measure that are in place.

This section consists of three parts:

1. Inbound Data Transfers
2. Internal Data Transfers
3. Outbound Data Transfers

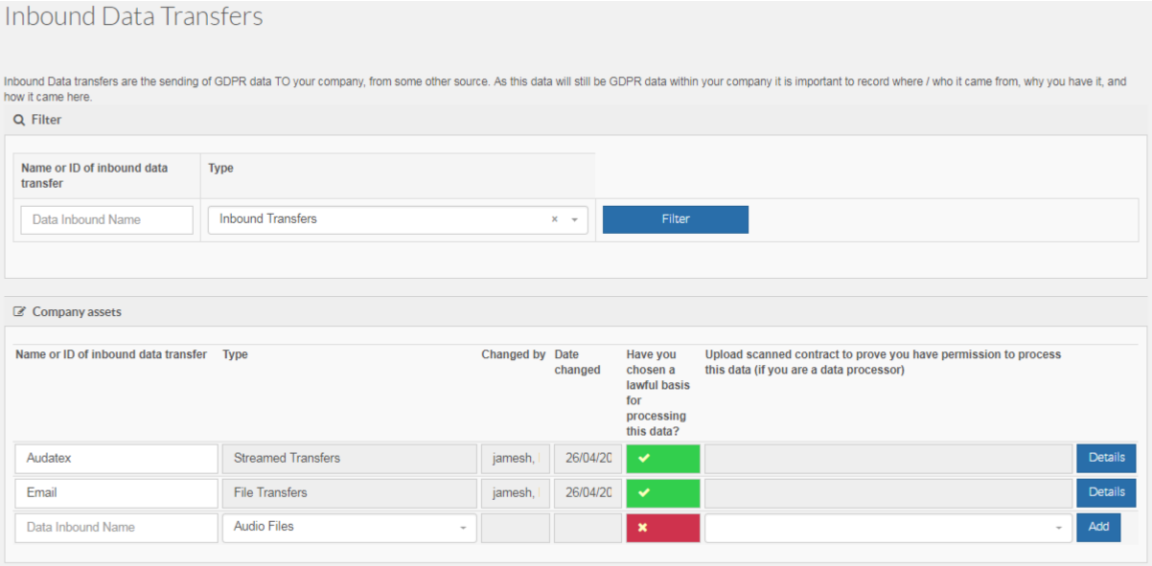
You will need to add details for each and every form of data transfer your business uses. This may include non-digital information e.g. paper-based files.

For specific details relating to electronic data, you may need to consult with your IT provider / web developer.

Inbound Data Transfers

Inbound Data Transfers are the sending of information TO your business i.e. the data you receive. You will need to know where / who it came from, why you have it and how it got there.

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of Inbound Data Transfers.



Inbound Data Transfers

Inbound Data transfers are the sending of GDPR data TO your company, from some other source. As this data will still be GDPR data within your company it is important to record where / who it came from, why you have it, and how it came here.

Filter

Name or ID of inbound data transfer	Type	
Data Inbound Name	Inbound Transfers × ▾	Filter

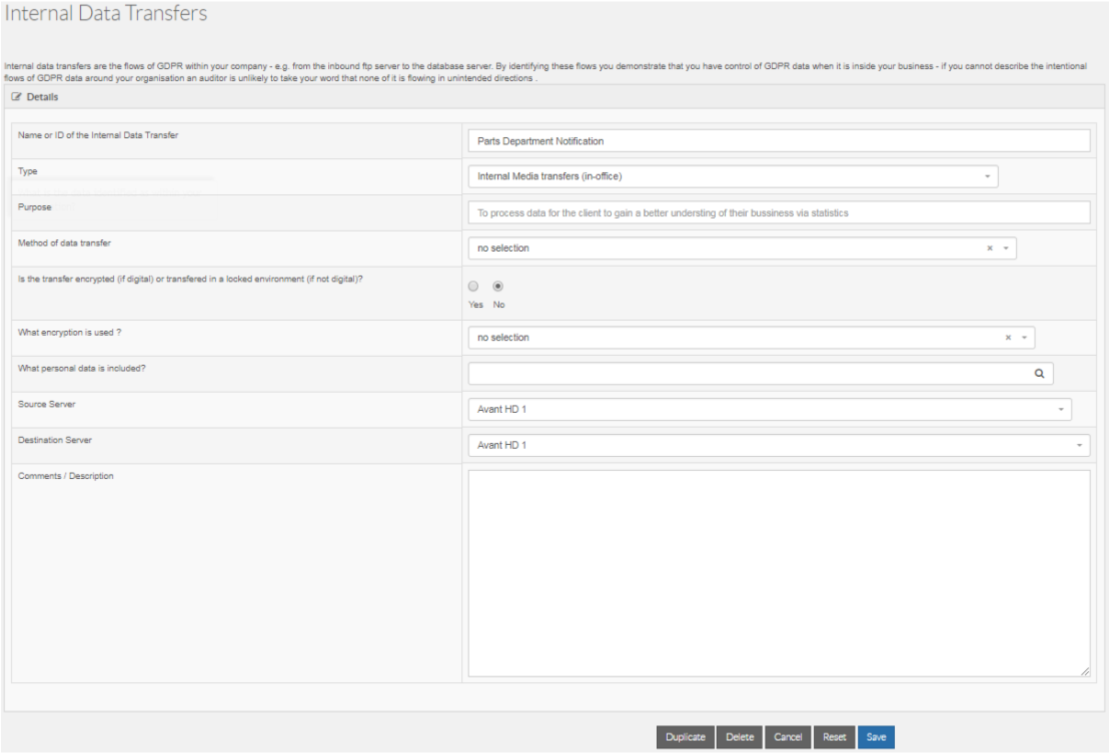
Company assets

Name or ID of inbound data transfer	Type	Changed by	Date changed	Have you chosen a lawful basis for processing this data?	Upload scanned contract to prove you have permission to process this data (if you are a data processor)	
Audatex	Streamed Transfers	jamesh,	26/04/20	✓		Details
Email	File Transfers	jamesh,	26/04/20	✓		Details
Data Inbound Name	Audio Files ▾			✗	▾	Add

Below the search facility is a list of the Inbound Data Transfers you will have added. At the bottom of the screen you are able to add (further) Inbound Data Transfers.

To add an entry, give the Inbound Data Transfer a unique name, then state type of transfer from the drop down menus provided and click “Add” (Add). From here you can also see that you have chosen a lawful basis for processing this data.

Once added, you can click on the “Details” (Details) button to add further information about the Inbound Data Transfer, including encryption details, what sort of personal information is included and who can access the data.



Internal Data Transfers

Internal data transfers are the flows of GDPR within your company - e.g. from the inbound ftp server to the database server. By identifying these flows you demonstrate that you have control of GDPR data when it is inside your business - if you cannot describe the intentional flows of GDPR data around your organisation an auditor is unlikely to take your word that none of it is flowing in unintended directions .

Details

Name or ID of the Internal Data Transfer	Parts Department Notification
Type	Internal Media transfers (in-office)
Purpose	To process data for the client to gain a better understing of their bussiness via statistics
Method of data transfer	no selection
Is the transfer encrypted (if digital) or transfered in a locked environment (if not digital)?	○ Yes ● No
What encryption is used ?	no selection
What personal data is included?	
Source Server	Avant HD 1
Destination Server	Avant HD 1
Comments / Description	

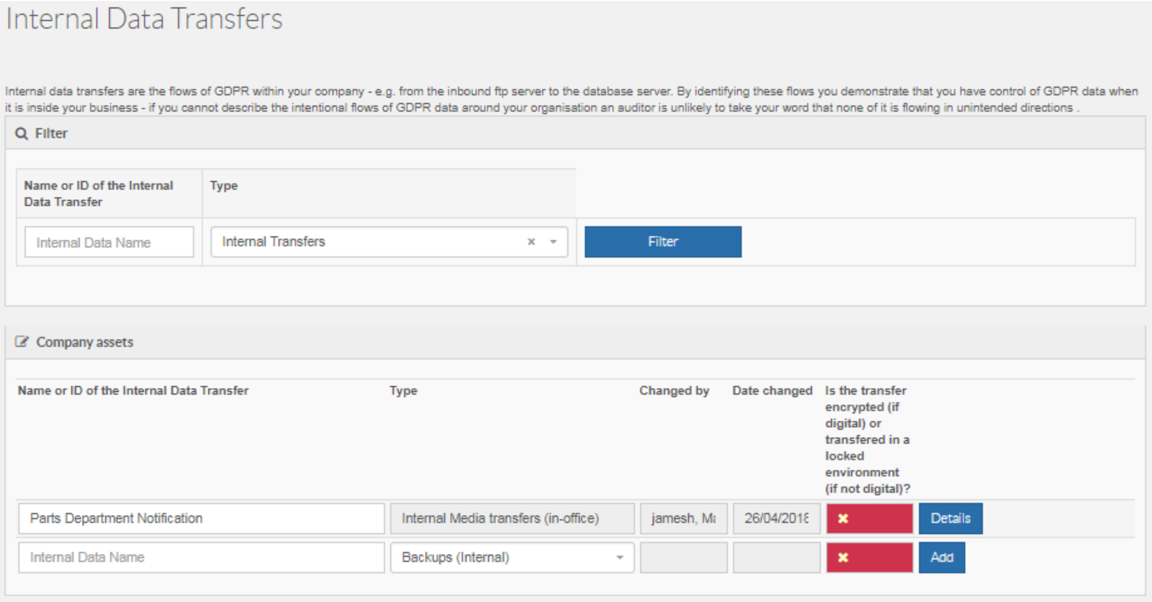
Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

Internal Data Transfers

Internal Data Transfers are the flows of data within your company e.g. from your ftp server to your database server. By identifying these flows you demonstrate that you have control of your personal data when it is inside your business

In this section you will need to list all types of Internal Data Transfers.

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of internal Data Transfers.



Internal Data Transfers

Internal data transfers are the flows of GDPR within your company - e.g. from the inbound ftp server to the database server. By identifying these flows you demonstrate that you have control of GDPR data when it is inside your business - if you cannot describe the intentional flows of GDPR data around your organisation an auditor is unlikely to take your word that none of it is flowing in unintended directions .

Filter

Name or ID of the Internal Data Transfer	Type	
Internal Data Name	Internal Transfers ×	Filter

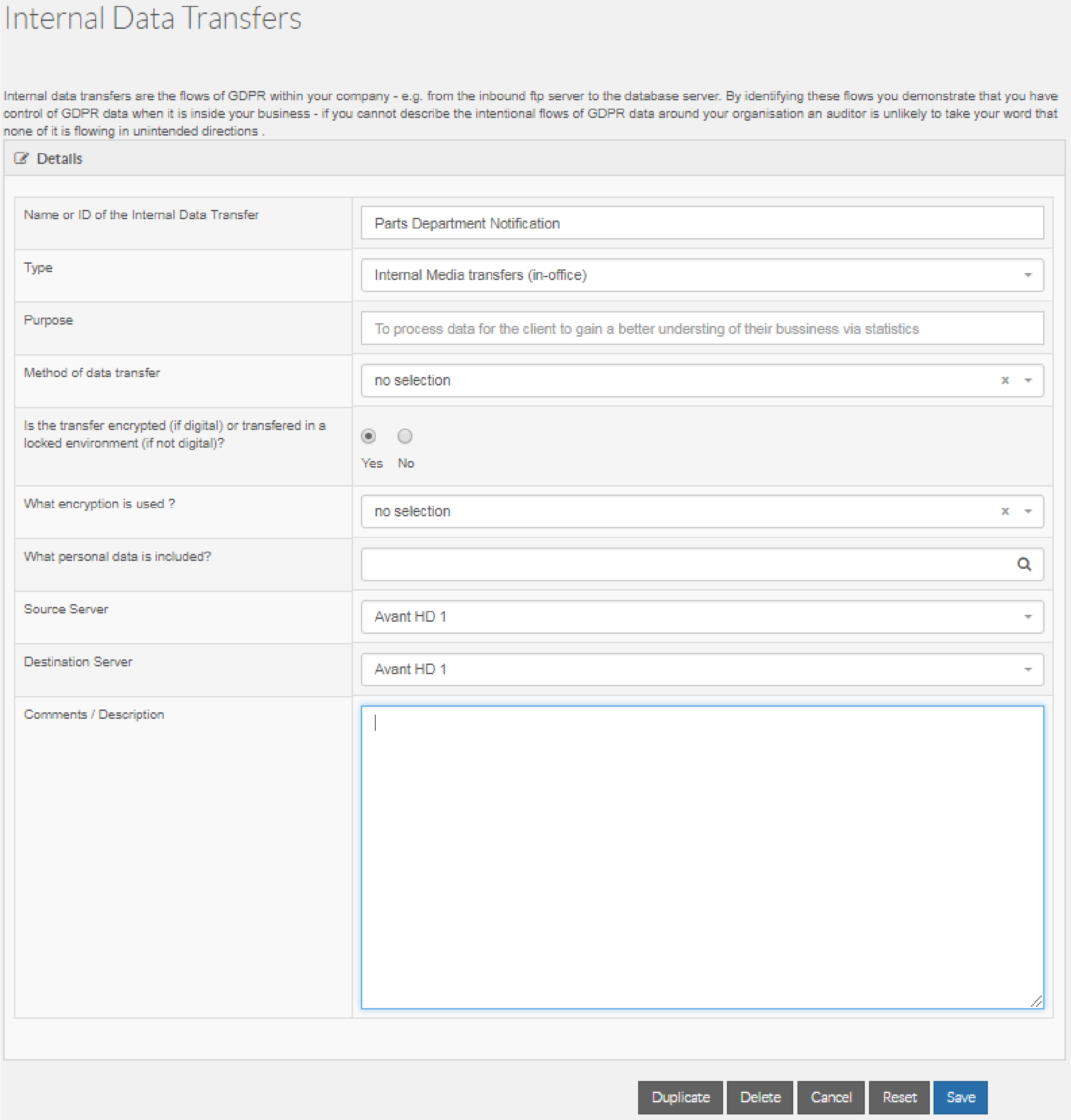
Company assets

Name or ID of the Internal Data Transfer	Type	Changed by	Date changed	Is the transfer encrypted (if digital) or transfered in a locked environment (if not digital)?	
Parts Department Notification	Internal Media transfers (in-office)	jamesh, Mi	26/04/2018	✖	Details
Internal Data Name	Backups (Internal)			✖	Add

Below the search facility is a list of the Internal Data Transfers you will have added. At the bottom of the screen you are able to add (further) Inbound Data Transfers.

To add an entry, give the Internal Data Transfer a unique name, then state type of transfer from the drop down menus provided and click “Add” (Add). From here you can also see if the transfer is encrypted.

Once added, you can click on the “Details” (Details) button to add further information about the Internal Data Transfer, including encryption details and where it goes.



Internal Data Transfers

Internal data transfers are the flows of GDPR within your company - e.g. from the inbound ftp server to the database server. By identifying these flows you demonstrate that you have control of GDPR data when it is inside your business - if you cannot describe the intentional flows of GDPR data around your organisation an auditor is unlikely to take your word that none of it is flowing in unintended directions .

Details

Name or ID of the Internal Data Transfer	Parts Department Notification
Type	Internal Media transfers (in-office)
Purpose	To process data for the client to gain a better understing of their bussiness via statistics
Method of data transfer	no selection
Is the transfer encrypted (if digital) or transfered in a locked environment (if not digital)?	● Yes ○ No
What encryption is used ?	no selection
What personal data is included?	
Source Server	Avant HD 1
Destination Server	Avant HD 1
Comments / Description	

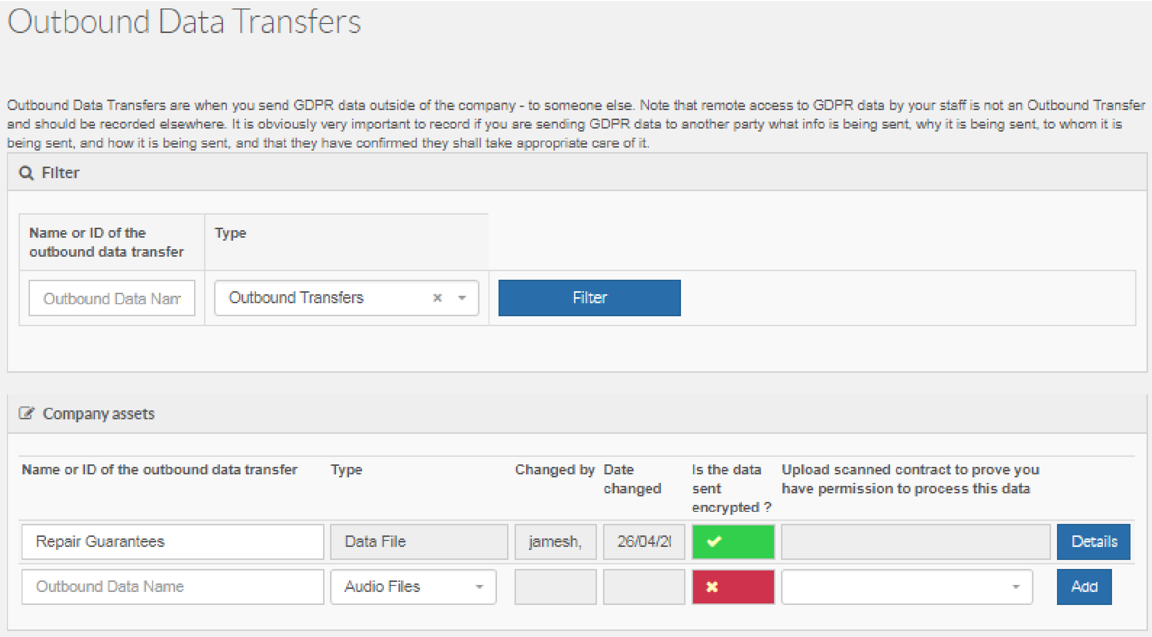
Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

Outbound Data Transfers

Outbound Data Transfers refers to the information you send to other businesses.

In this section you will need to list all types Outbound Data Transfers.

At the top of this section is a search facility (Filter). This will be useful once you have created a full list of Inbound Data Transfers.



Outbound Data Transfers

Outbound Data Transfers are when you send GDPR data outside of the company - to someone else. Note that remote access to GDPR data by your staff is not an Outbound Transfer and should be recorded elsewhere. It is obviously very important to record if you are sending GDPR data to another party what info is being sent, why it is being sent, to whom it is being sent, and how it is being sent, and that they have confirmed they shall take appropriate care of it.

Filter

Name or ID of the outbound data transfer	Type	
Outbound Data Narr	Outbound Transfers ×	Filter

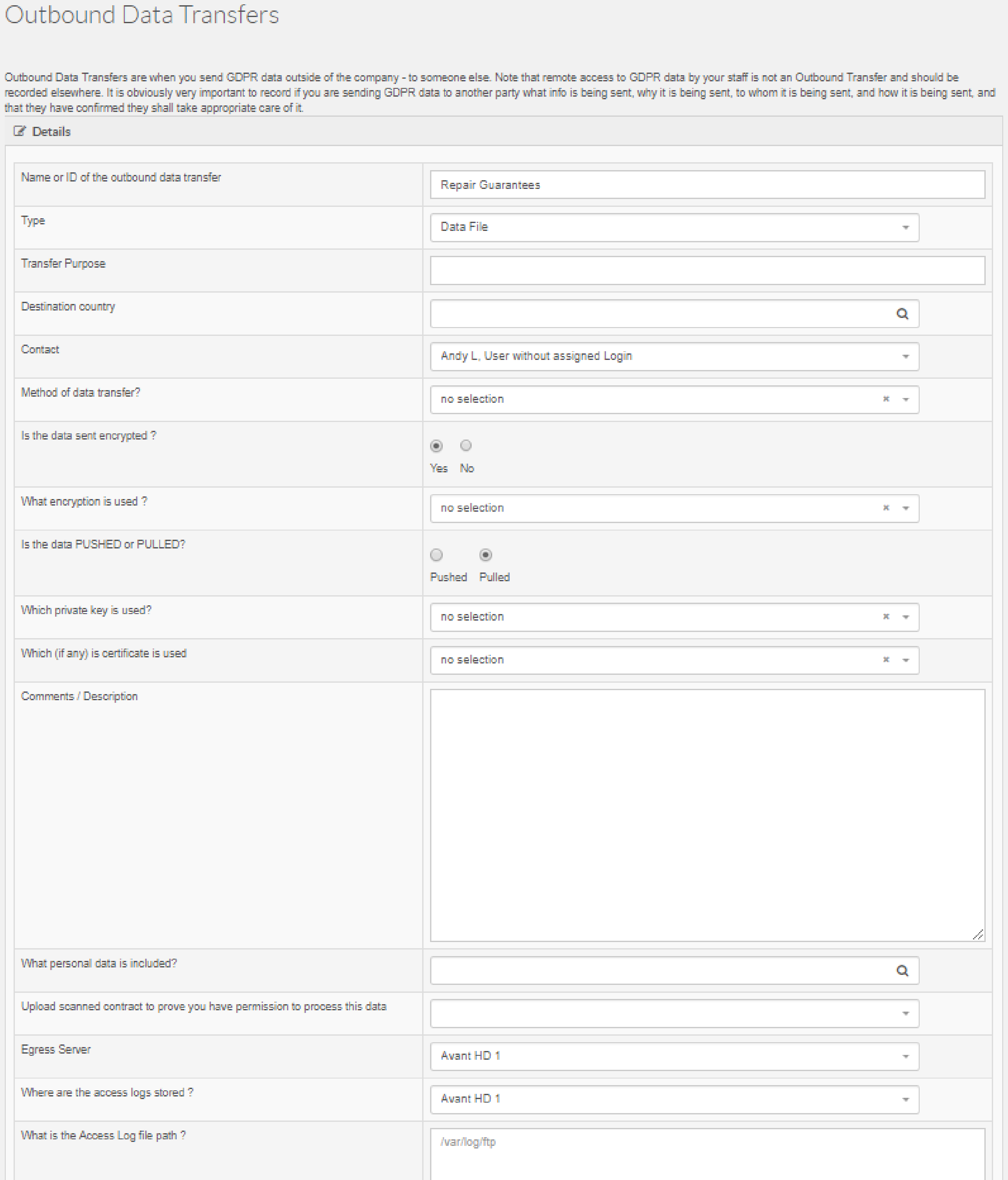
Company assets

Name or ID of the outbound data transfer	Type	Changed by	Date changed	Is the data sent encrypted ?	Upload scanned contract to prove you have permission to process this data	
Repair Guarantees	Data File	jamesh,	26/04/2(	✓		Details
Outbound Data Name	Audio Files			✖		Add

Below the search facility is a list of the Outbound Data Transfers you will have added. At the bottom of the screen you are able to add (further) Outbound Data Transfers.

To add an entry, give the Outbound Data Transfer a unique name, then state type of transfer from the drop down menus provided and click "Add" (Add). From here you can also see if the transfer is encrypted.

Once added, you can click on the "Details" (Details) button to add further information about the Internal Data Transfer, including encryption details, access logs and transfer methods.



Outbound Data Transfers

Outbound Data Transfers are when you send GDPR data outside of the company - to someone else. Note that remote access to GDPR data by your staff is not an Outbound Transfer and should be recorded elsewhere. It is obviously very important to record if you are sending GDPR data to another party what info is being sent, why it is being sent, to whom it is being sent, and how it is being sent, and that they have confirmed they shall take appropriate care of it.

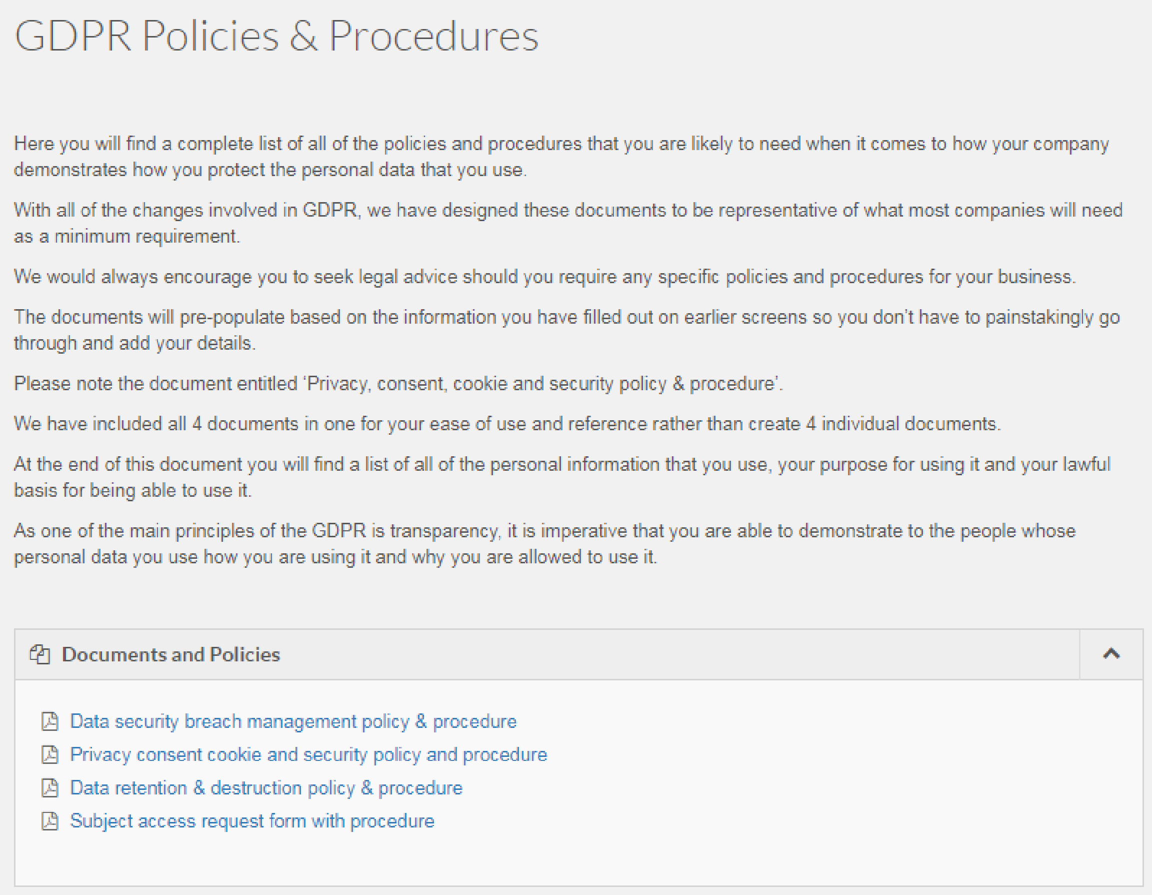
Details

Name or ID of the outbound data transfer	Repair Guarantees
Type	Data File
Transfer Purpose	
Destination country	
Contact	Andy L, User without assigned Login
Method of data transfer?	no selection
Is the data sent encrypted ?	● Yes ○ No
What encryption is used ?	no selection
Is the data PUSHED or PULLED?	○ Pushed ● Pulled
Which private key is used?	no selection
Which (if any) is certificate is used	no selection
Comments / Description	
What personal data is included?	
Upload scanned contract to prove you have permission to process this data	
Egress Server	Avant HD 1
Where are the access logs stored ?	Avant HD 1
What is the Access Log file path ?	/var/log/ftp

Once this information is complete, remember to click “Save” (Save) to update the record. This will then return you to the previous screen.

GDPR Policies

In this section you will find a complete list of all of the policies and instructions that you are likely to need when it comes to your company's personal data protection.



GDPR Policies & Procedures

Here you will find a complete list of all of the policies and procedures that you are likely to need when it comes to how your company demonstrates how you protect the personal data that you use.

With all of the changes involved in GDPR, we have designed these documents to be representative of what most companies will need as a minimum requirement.

We would always encourage you to seek legal advice should you require any specific policies and procedures for your business.

The documents will pre-populate based on the information you have filled out on earlier screens so you don't have to painstakingly go through and add your details.

Please note the document entitled 'Privacy, consent, cookie and security policy & procedure'.

We have included all 4 documents in one for your ease of use and reference rather than create 4 individual documents.

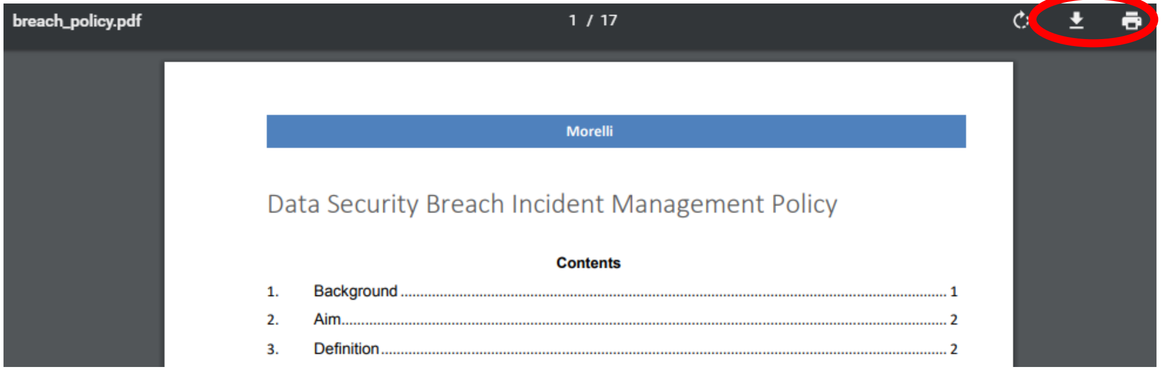
At the end of this document you will find a list of all of the personal information that you use, your purpose for using it and your lawful basis for being able to use it.

As one of the main principles of the GDPR is transparency, it is imperative that you are able to demonstrate to the people whose personal data you use how you are using it and why you are allowed to use it.

Documents and Policies
Data security breach management policy & procedure
Privacy consent cookie and security policy and procedure
Data retention & destruction policy & procedure
Subject access request form with procedure

The information completed in the previous sections will auto-populate within the documents. Simply click on the name of the policy you wish to view and it will open within your web browser as a PDF.

You can print or download a copy of the documentation by clicking on the icons in the top right corner of the web page, highlighted in the red circle below.



Morelli

Data Security Breach Incident Management Policy

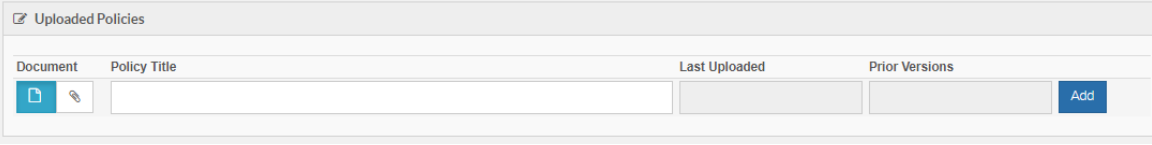
Contents

The GDPR Systems OFFICE GPDR solution will provide you with the following documents:

- Data security breach management policy & procedure
- Privacy, consent, cookie and security policy and procedure
- Data retention & destruction policy & procedure
- Subject access request form with procedure

It is your responsibility to read through these documents so you can action them or refer to them as needed.

In addition, you are also able to upload your own documentation, to ensure everything relating to Data Protection is stored securely within the same area.



Uploaded Policies

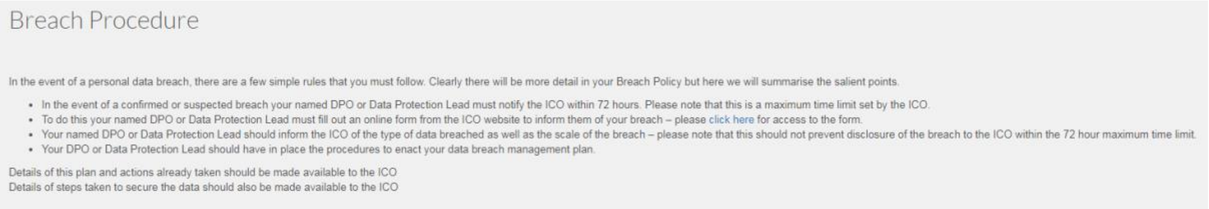
Document	Policy Title	Last Uploaded	Prior Versions	
				Add

To do this click on the paper clip icon (📎) to open your document folders, navigate to the required policy and press the “Open” button (Open). Then give the policy a suitable name within the Policy Title field and press “Add” (Add) to add to the system.

Personal Data Breach Procedure

This section provides you with information regarding what you should do in the event of a data breach.

The system is not able to prevent a breach taking place. However, by completing all the sections within the system you will have the policies and documented procedures to prove that you have done everything within reason to protect your personal data.



Breach Procedure

In the event of a personal data breach, there are a few simple rules that you must follow. Clearly there will be more detail in your Breach Policy but here we will summarise the salient points.

- In the event of a confirmed or suspected breach your named DPO or Data Protection Lead must notify the ICO within 72 hours. Please note that this is a maximum time limit set by the ICO.
- To do this your named DPO or Data Protection Lead must fill out an online form from the ICO website to inform them of your breach – please click here for access to the form.
- Your named DPO or Data Protection Lead should inform the ICO of the type of data breached as well as the scale of the breach – please note that this should not prevent disclosure of the breach to the ICO within the 72 hour maximum time limit.
- Your DPO or Data Protection Lead should have in place the procedures to enact your data breach management plan.

Details of this plan and actions already taken should be made available to the ICO
Details of steps taken to secure the data should also be made available to the ICO