TEAM Software by WORKWAVE

Data Protection Tool Kit

GDPR Principles & Pointers

20 September 2021

COMMERCIAL STATEMENT

This document is subject to any terms as per teamsoftware.com/legal.

HELPDESK & SUPPORT

For help and support, please contact TEAM Software Technical Support:

- **Opening hours:** 8am -5pm Monday - Friday (excluding weekends and public holidays)
- **Contact telephone number:** 0370 626 0400 (then press option 1)
- **Email:** support@innovise.com

DOCUMENT CONTROL

Version History

Version Number	Revision Date	Summary of changes (List the reason for each version of the document)	Author(s)
1801-001	01/05/2018	Initial release of document	Keith Williams, Paul Newman, Neil Barlow and Mike Taylor
1802-001	21/05/2018	Updated guide to coincide with 18.2 release	Keith Williams and Paul Newman
1802-002	05/05/2018	Updated Innovise contact details	Keith Williams
2101-001	19/01/2021	Updated into TEAM Software format	Keith Williams

TABLE OF CONTENTS

INTRODUCTION

What's this guide all about?

From Friday 25 May 2018, processing of personal data by organisations will have to comply with the General Data Protection Regulations. The regulations set out a series of rules that amongst other things detail:

- What can be stored (in terms of content, need and relevancy)
- What can be shared (and with whom)
- How data can be collected, stored lawfully and used
- How long data can be kept
- The rights of an individual regarding the personal data held about them

For all companies handling individual's data, these new regulations will have an impact on the way in which they acquire, store, process and dispose of their content. As a TEAM Software customer, it is highly likely that you will be holding this type of data on your TEAM Software system(s). This guide will advise you of the tools that we have built into our software products to help you in your GDPR compliance activities.

Which TEAM Software areas are affected by GDPR and how?

All areas of the Timegate solution family are affected. This includes the Recruit Pack (comprising the product elements known as PASS, PDC and OLR). The level of the impact and changes needed is dependent upon the specific area as detailed in the table below:

Area	Initial impact/changes/set up
Timegate Web	• The Timegate web client is used to set up the main GDPR settings. This is done through the Admin | System | System Settings | Data Protection tab. These settings control GDPR features for Timegate/PASS, although some products will need further configuration • Supports the audit of changes to Employee consent for sensitive data
Timegate Desktop	• This application is not being modified. GDPR configuration is managed exclusively in the Web Client
Timegate Services	• Automated processes to remove data in line with retention laws
Employee Portal	• Initial contact emails could be modified to include Data Protection Link • The header of the Employee Portal will support a link to your Data Protection Policy
PASS Client	• You could update your templates with a Data Protection Link. We have provided merge fields that you may wish to use to do this • New features are provided to support Candidate consent for sensitive data where it is collected (optional configuration)
PASS Services	• Automated processes to remove data in line with retention laws

PDC Portal	• You could update your email templates with a Data Protection Link and your Retention Consent Wording. We have provided merge fields that you may wish to use to do this. You may use these in screening type text • The header of the website will automatically be modified to include your Data Protection Link • Your retention of data and sensitive data consent message will automatically be shown on the Candidate's Personal Information page • New features are provided to support Applicant consent for sensitive data if it is asked for and configured • You could configure your data retention settings to your internal policies for PDC data
OLR Portal	• The header of the OLR website will automatically include a link to your Data Protection Policy. Your Retention Consent Wording will also be displayed • You should ask TEAM Software if you would like to update your templates with a Data Protection Link and your Retention Consent Wording

Which GDPR features are supported by our systems?

GDPR Feature	Timegate Web	Timegate Services	Employee Portal	PASS Client	PASS Services	PDC Portal	OLR Portal
Data Protection Set Up Tab	✓						
The Your Rights Link			✓	✓		✓	✓
Retention Consent				✓		✓	
Sensitive Data Consent	✓			✓		✓	
Retention Policies	✓	✓	✓	✓	✓	✓	✓

Please Note:

- The Sensitive Data Consent changes made by TEAM Software do not cover **User Defined Fields (UDFs)**. You could check any **UDFs** to ensure that you are not holding any sensitive data that you do not have consent for, making appropriate changes to ensure compliance
- Should you need to delete data that is not easily achieved through the existing User Interface, please contact your TEAM Software representative

DATA PROTECTION SET UP

Follow the steps below to find and set up Data Protection when you are signed into Timegate's Web Client:

1. Sign in to Timegate and select Admin from the menu ribbon at the top of the page
2. From the sub menu, select System
3. The system's **Admin | System | System Settings | Absence General** tab should be displayed. Select the ⓘ beside **Data Protection** from the menu on the left most side of the screen
4. Set up the individual values listed on the **Data Protection tab**. Details of how to configure these settings are covered over the next few sections of this guide
5. Once set up, select **Save**

THE YOUR RIGHTS LINK

What's the Your Rights Link? Why is it important?

GDPR Key Points:

- Organisations are required to detail and publish their Data Protection Policy
- You must inform individuals about the collection and use of their personal data on first contact (i.e. before or as soon as they arrive on your website)
- All communications about Data Protection should be clear and easy to understand
- The Your Rights Link (that links to your Data Protection Policy) should be available on external facing websites where you're collecting data

Within TEAM Software's systems, the Your Rights Link gives you the opportunity through a direct hyperlink, to provide individuals with details of their Data Protection Rights, when they first contact your company. Potentially this could be through an email, a letter or on your system's website(s). Please note that the page holding your policy statement is not included in the Timegate solution. You will need to host this on a publicly accessible website for this to be accessed using the hyperlink features.

How's it set up?

General set up

The **Your Rights Link** is created using two values - the **Data Protection Link** and the **Data Protection Message**. The link is used for website hyperlinks and for use in templates. The two values can be set up from Timegate's z

1. Enter the destination of the **Data Protection Link**. This is the URL (website address) that will link to your **Data Protection Policy**. You are responsible for the hosting of this file. It will not be hosted on your Timegate system. By default this value will be left blank as TEAM Software are unable to complete your URL for you. An example of this value could be: **http://www.yourcompany.com/data-protection-policy.pdf**
2. Enter your **Data Protection Message**. This message is the wording that will appear on the hyperlink that takes the user to your **Data Protection Policy**. Your system users will click on this when it is displayed, to view your **Data Protection Policy**. By default, this value will be left blank. An example of this value could be: **Click here to view our Data Protection Policy**

PASS specific set up

In PASS, the values in the **Data Protection Message** and **Data Protection Link** fields (that were set up above) have been assigned to the merge fields letting you use the **Your Rights Links** within Candidate reports and chase email templates as follows:

- **<<Data_Protection_Policy_Message>>** - the value defined in Data Protection Message
- **<<Data_Protection_Policy_URL>>** - the value defined in Data Protection Link

The fields are supported in the following areas:

- **Simple Candidate Report Template**
- **Detailed Candidate Report Template**
- **Reference Chase Email**
- **Quick Comments Maintenance**

Want more information? Please see Deployment Guide – PASS – GDPR - Merge fields (IS-DG-PS1801-001)

PDC specific set up

In PDC, the values in the Data Protection Message and Data Protection Link fields will be used to automatically update the website header for you, with the Your Rights Link. The values in the two fields have also been assigned to a HTML merge field letting you use the Your Rights Link within the First Chase, Subsequent Chase and Final Chase Email templates. The following code could be used which will generate the Your Rights Link:

```
<pdcdata area="system" value="GDPRLink"/>
```

To simplify this process, HTML similar to the following could be added to the bottom of existing templates. This will add a line (horizontal rule) under the email body, and then create the Your Rights Link:

```
<hr />
<p><pdcdata area="system" value="GDPRLink"/></p>
```

Want more information? Please see Deployment Guide – PASS – GDPR – Your Rights Link in PDC and OLR (IS-DG-PS1801-002)

OLR specific set up

In OLR (“Online Referencing”), the values in the **Data Protection Message** and **Data Protection Link** fields will be used to automatically update your website with the **Your Rights Link**. Outbound email templates, however, need to be set up. This is not something that you can do yourself. Please speak to us regarding the format of your changes, so that we can arrange for this to be set up on your behalf.

Want more information? Please see Deployment Guide – PASS – GDPR – Your Rights Link in PDC and OLR (IS-DG-PS1801-002)

Employee Portal specific set up

In the Employee Portal, the values in the **Data Protection Message** and **Data Protection Link** fields will be used to automatically update your website with a link to your **Data Protection Policy**. The **Your Rights Link** is shown as a shield icon in the header of the portal. The website link is that which is defined in the **Data Protection Link** field. When viewed on a web-browser supporting roll-over text, the **Data Protection Message** field is displayed when a mouse is rolled on to the shield icon. Additionally, the two values have been combined into a merge field called **Data Protection Link** for use within email templates (such as the **Password Email** that is sent on first contact).

Want more information? Please see Please contact your TEAM Software support team

RETENTION CONSENT

What's Retention Consent? Why is it important?

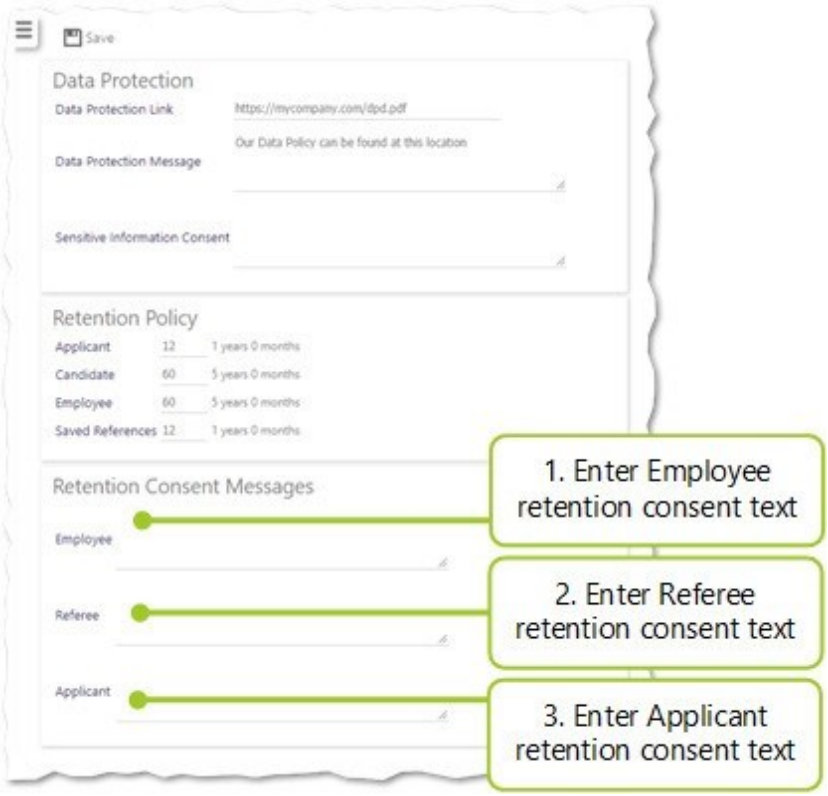
GDPR Key Points:

- Organisations are required to display a retention consent message to users before their data is collected. The message should inform users that you will be retaining their data along with the ways in which you will be using it
- The GDPR sets a high standard for consent. It offers individuals a real choice and control over how their data is used (i.e. it requires a positive opt-in and puts the individual in charge)
- Explicit consent requires a very clear and concise but specific statement of consent, that is kept separate from other terms and conditions

The Retention Consent Messages give you the opportunity to provide individuals (be they Employees, Referees or Applicants) with a statement of consent that they will see as they access the web pages used to enter data.

How's it set up?

The three **Retention Consent Messages** can be set up from Timegate's **Admin | System | System Settings | Data Protection tab** in 18.2:



1. Enter your **Retention Consent Messages (Employee)**. This wording forms the consent message that will appear on the Employee Portal. You should seek legal guidance for the wording that is appropriate to your organisation
2. Enter your **Retention Consent Messages (Referee)**. This wording forms the consent message that will appear on the OLR page presented to the Referee. It is also available as a mail merge field to be used in

Referee templates. The default value for this will be blank. You should seek legal guidance for the wording that is appropriate to your organisation

3. Enter your **Retention Consent Messages (Applicant)**. This wording forms the consent message that will appear on the PDC Applicant page and is available as a mail merge field for use in Applicant templates. The default value for this will be blank. You should seek legal guidance for the wording that is appropriate to your organisation

Want more information? Please see Deployment Guide – PASS – GDPR – Retention Consent Wording" (IS-DG-PS1801-003)

Please Note: If you are still using 18.1 and would like to make use of this functionality in the Recruit Pack's PDC or OLR, please contact your TEAM Software Technical Support Team. These settings will need to be configured by the support team on your behalf.

PASS specific set up

The values in two of the Retention Consent Message fields (that were set up above) have been assigned to a merge field for use within Candidate reports and quick comments:

- **<<Retention Consent Message_Applicant>>** - the value defined in Applicant
- **<<Retention Consent Message_Reference>>** - the value defined in Referee

The fields are supported in the following areas:

- **Simple Candidate Report Template**
- **Detailed Candidate Report Template**
- **Reference Chase Email**
- **Quick Comments Maintenance**

Want more information? Please see Deployment Guide – PASS – GDPR - Retention Consent Merge fields (IS-DG-PS1802-001)

PDC specific set up

The value in the Applicant field will be used to automatically update the Personal Information page of the website for you. The message will be displayed at the top of the Personal Information page. The value has also been assigned as a HTML merge field for your use, within any screening type text area or within an email template. The following code could be used which will display the content of the Applicant field:

```
<pdcdata area="system" value="RetentionConsentMessage_Applicant"/>
```

Want more information? Please see Deployment Guide – PASS – GDPR – Retention Consent Wording (IS-DG-PS1801-003)

OLR specific set up

The value in the Referee field will be used to automatically update the website for you with your Referee text. Although it is not necessary, you may wish to have outgoing emails or page templates to include the Referee text. This is not something that you can do yourself. Please speak to us regarding the format of your changes, so that we can arrange for this to be set up on your behalf.

Want more information? Please see Deployment Guide – PASS – GDPR – Retention Consent Wording (IS-DG-PS1801-003)

Employee Portal specific set up

In the Employee Portal, the values in the Employee field will be used to automatically update the website for you, with your company's message. When an employee selects the pencil button, to update their details, the message is displayed on the update details screen. The message is shown when the Employee updates their Employee image, their name, their Address or their HR details within the Employee Portal (if they have the option to make changes).

SENSITIVE INFORMATION CONSENT

What's Sensitive Information Consent? Why is it important?

GDPR Key Points:

- Processing of personal data that is described as sensitive is subject to specific requirements that exceed those for non-sensitive data
- This special, sensitive data includes (but is not limited to) information about an individual's race, ethnic origin, religion, biometrics (where used for identification purposes) and health. There are fields in Timegate and PASS that support information of this type and therefore, additional features have been added relevant to these data sets

The Sensitive Information Consent field within TEAM Software systems gives you the opportunity to explain to individuals their rights around providing information to your business. It enables you to explain how you will use their data if they consent.

A tick box will be provided, which if not selected will result in any stored data from the affected fields being removed.

Any changes to sensitive information on the system will be tracked and will be fully audited to ensure compliance. When your systems are upgraded to 18.2 or above, the records of all Applicants, Candidates and Employees who have given consent already will be tagged in the audit record as "Consent given pre-GDPR". Any changes made thereafter to records, will be listed in the audit records, along with details about how the consent was gained and the time/date of the change.

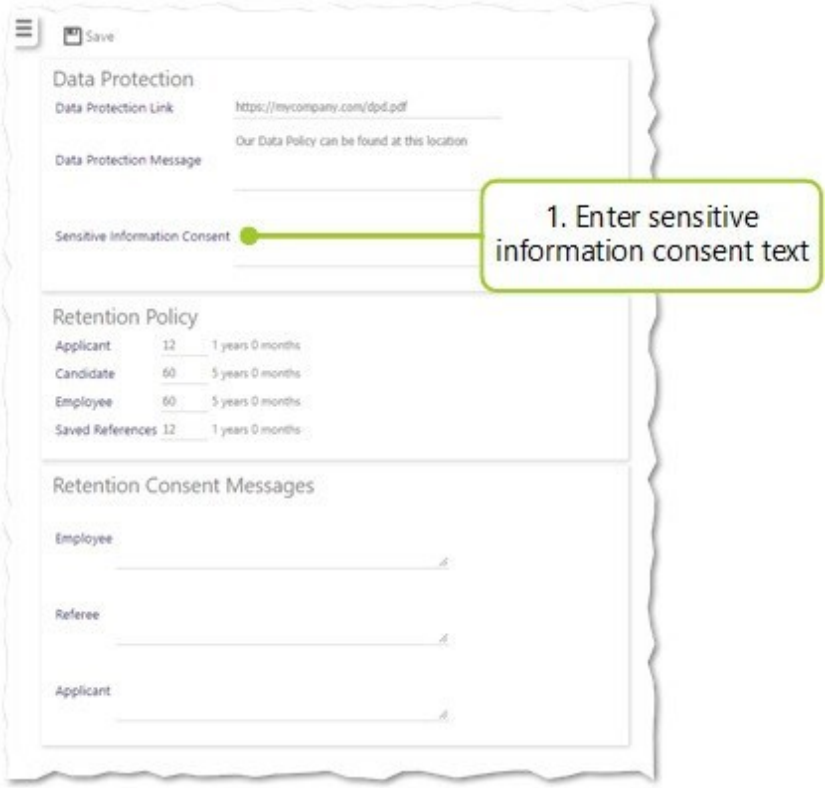
The following table explains how **Sensitive Information Consent** will be handled within your TEAM Software systems:

Sensitive Information	How Handled within TEAM Software Systems
Ethnic Origin	• Requires consent from the individual
Religion	• Requires consent from the individual
Sexual Orientation	• Requires consent from the individual
Considered Disabled/Disabled Details	• Requires consent from the individual
Biometric Data	• Finger-scan data is held locally on the terminals used to clock on / off that support biometric authentication • On stand-alone terminals, there is no other identifying information stored with the fingerprints unless you choose to add it through the user interface. It is your responsibility to review your set up and ensure compliance with the GDPR provisions related to Biometric Data • If you use grouped devices, it's your responsibility to ensure compliance. You could take advice on whether you have a lawful justification for holding biometric data centrally, which is how templates are shared for grouped devices
Other Forms Of Sensitive Data (e.g. Health Or Trade Union Membership)	• There are no standard fields to hold this information. However, your system may have been configured so that it stores this type of information using User Defined Fields (UDFs). You will need to check any UDFs and change them to ensure that your company's

	compliance • Additionally, this kind of information may be gathered by reference. To ensure your company's compliance, you could adjust your screening

How's it set up?

The following value can be set up from Timegate's **Admin | System | System Settings | Data Protection tab** in Timegate 18.2:



1. Enter your Sensitive Information Consent text. This message is the consent message wording that will appear on your TEAM Software system websites and in templates. By default, this value will be left blank. You may wish to seek legal guidance for the wording that is appropriate to your organisation

PDC specific set up

The value in the Sensitive Information Consent field will be displayed automatically above the Equal Opportunities section of the Personal Information page if your configuration includes this in the screening type. The message will be accompanied with the consent check box.

Want more information? Please see "Deployment Guide – PDC – GDPR Sensitive Data Consent" (IS-DG-PS1802-001)

PASS specific set up

A check box will be added to the Candidate details page indicating if consent is given and at what date/time. The system user will need to detail how they obtained consent from the Candidate, if they make changes to their sensitive information. Meanwhile, behind the scenes, the system will handle such auditing changes, along with clearing down records, based on the consent details provided, as necessary.

Timegate specific set up

You will not need to do anything in Timegate to configure the system. A check box will be added to the Employee details in the Set Up | Employee | HR tab. This is used to indicate whether consent is given and if so, at what date/time. You will need to detail how you obtained consent from the Candidate, if you make changes to their sensitive information.

Meanwhile, behind the scenes, the system will handle such auditing changes along with clearing down records based on the consent details provided, as necessary.

Want more information? Please see Please contact your TEAM Software Technical Support Team

Please Note: The Timegate Desktop Client is not being modified by TEAM Software to ensure GDPR compliance. You will need to ensure that your staff are using the Web Client if you are using Sensitive Data Fields

RETENTION POLICIES

What are Retention Policies? Why are they important?

GDPR Key Points:

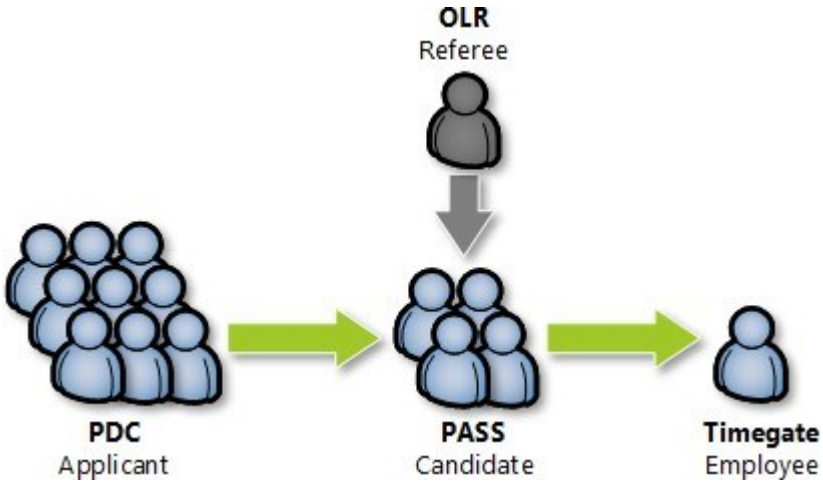
- As a general rule of thumb, an individual's data should only be retained for as long as necessary for the purpose of processing
- This period will differ from business to business and is dependent upon the type of data processed and the purpose of processing. You will need to determine your retention policies

Retention Policies are used to set an automated process that will remove data that it is no longer lawful for your organisation to hold.

You can set up a series of five retention policy date rules from within Timegate (detailed below) that will be used to determine when the system's automated routines will remove an individual's data. Whenever this happens, an audit table will be created automatically. This tracks how many records have been removed along with the details of the record type (e.g. Referee, Applicant, Candidate or Employee) and when the removal took place.

When content is removed (based on the retention policy date), the data is either deleted or obfuscated depending upon the specific data element. In addition to the data stored in records, physical documents relating to the individual will be deleted.

Please Note: Retention is based on the principal where by an individual's record moves through the various TEAM Software systems as illustrated below:

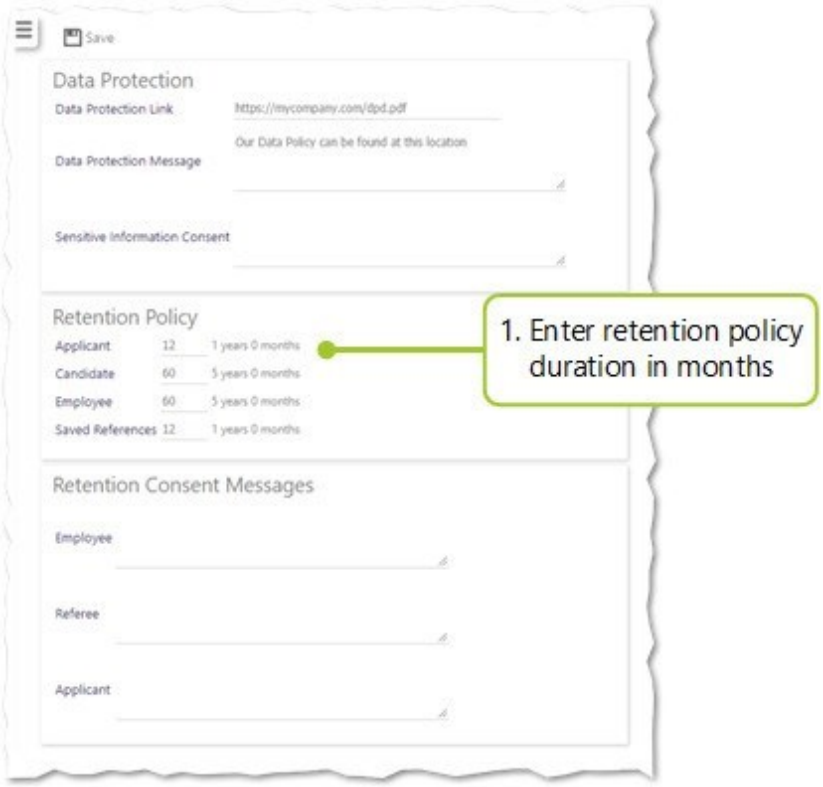


At each stage, the individual's details will be removed, unless they have been successful and moved on to the next stage in the Applicant-Candidate-Employee process.

For example, an Applicant's details will be removed unless the Applicant becomes a Candidate. A Candidate's details will be removed unless the Candidate becomes an Employee.

How are they set up?

The following value can be set up from Timegate's **Admin | System | System Settings | Data Protection** tab in Timegate 18.2:



1. In this section, you can set up the duration (in months) that your organisation plans to keep data. By default, the values are those shown above, however, you could change these to meet your needs. The retention policy choices are listed below along with the actions undertaken when the date specified is reached:

    - **Retention Policy Saved References** – delete all reference data after the number of months specified in the retention policy have elapsed. This period applies from the last time the Reference was updated.
    - **Retention Policy Applicant** – delete all data about Applicants including documents after the number of months specified in the retention policy have elapsed (unless they have become Candidates). This period applies from the Applicant creation date. Want more information? Please see “Deployment Guide – PASS – GDPR - Retention Policy” (PASS) (IS-DG-PS1802-003)
    - **Retention Policy Candidate** – delete all data about Candidate’s from the database, including physical documents and email trails after the number of months specified in the retention policy have elapsed (unless they have become Employees). This period applies from either the Candidate’s screening start date, screening restart date or their Candidate creation date (depending on which date they have with a value stored in it). Want more information? Please see “Deployment Guide – PDC – GDPR Retention Policy” (IS- DG-PS1802-004)
    - **Retention Policy Employee** – rows relating to Employees in tables are made unidentifiable from the individual. Any physical documents relating to the Employee are deleted after the number of months specified in the retention policy have elapsed. This period applies from the Employee’s terminated date.

Want more information? Please see “Deployment Guide – GDPR Consents and Policy Management” (IS-DG-TG1802-001)

Timegate, PASS and PDC specific set up

You may need to contact us for further help and support.

OLR specific set up

OLR already supports a global policy for how long it retains data after a reference has been completed (prior to being moved to an archive area) and then how long it is retained in archive before it is removed from the system altogether. As an individual's data within the Recruit Pack's OLR is transient, TEAM Software has ensured that these settings are appropriately low values.

Timegate API specific set up

The "old" Timegate API can be configured to store XML files containing personal data if it is being used. By default, logging is switched off. If it is switched on and used for troubleshooting, the data should only be retained for that period of time and deleted straight away. It is your responsibility to review your use of these features. Please contact your TEAM Software Technical Support Team for further help and support if it's required.

Custom SSIS packages and tables specific set up

If your company uses custom SSIS packages that store Employee Applicant data, you will need to contact us. We will then work with you to help you make sure that these packages are updated to respect retention policies. It is your responsibility to review your use of these features.

DATA REMOVAL

What's Data Removal? Why is it so important?

GDPR Key Points:

- Individuals have the right to have all of their data on your system(s) deleted, under certain circumstances. These circumstances may include if you are holding their data and it is no longer necessary or relevant for the purpose that you originally collected the data
- Data from individuals that withdraw their consent must be deleted (or obfuscated so that it does not link to their identity in any way)

What are TEAM Software doing to support Data Removal?

The current approach to this requirement is to delete records using the User Interface. We are planning to develop a Data Removal Wizard to enable specific data types to be removed or made anonymous. This will be available in a future release.

What do you need to do?

Please contact your TEAM Software Technical Support Team, if an individual makes a request that you remove their data and you're unable to achieve this using the normal delete features from the user interface.

ACCESS REPORTING

What's Access Reporting? Why is it so important?

GDPR Key Points:

- At any point in time, an individual has the right, in an electronic format, to be provided, free of charge the personal information that your organisation holds about them. This is known as a Subject Access Request (SAR)
- The information returned to them should be in a clear and intelligible form
- There is no specific electronic format mandated, however, it needs to be machine readable, structured and contain all their data

What are TEAM Software doing to support Access Reporting?

There are numerous reports available in Timegate, PASS and the Insights solution to support this requirement. You will need to consolidate several reports to satisfy the SAR.

What do you need to do?

If you need to access information that you cannot access via reports, please contact your TEAM Software Technical Support Team and we will provide you with assistance.