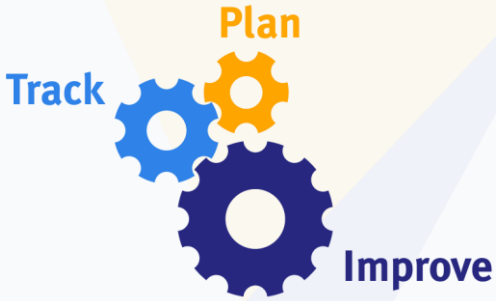
Timemaster

Administrator guidelines for processing personal data



Equisys Timemaster Ltd
Units 15B & 15C Marina Court
Castle Street
Kingston Upon Hull
East Yorkshire HU1 1TJ
United Kingdom

Tel: +44 (0)1482 588532

www.equisys.com

Contact: Support, **timemastersupport@equisys.com**

Contents

1. Introduction 3
1.1 What is GDPR? 3
1.2 Who does the GDPR affect? 3
1.3 What constitutes personal data? 3
1.4 Why should it concern you? 3
1.5 Document Scope 3
1.6 Disclaimer 3
2. What personal information is held within Timemaster? 4
Contact Details 4
Employment Details 4
Payroll 4
Accounting Interface 4
Additional Information 5
3. Informing staff of their GDPR rights 5
3.1 Auto prompting (Login Message) feature 5
4. How can staff view their own personal information you store in Timemaster? 5
4.1 My Details 5
5. Protecting access to personal data? 6
5.1 Controlling access to personal data. 6
Staff Related Functions 6
Reports 6
Report Restrictions 6
System Administration 7
5.2 Providing details of what personal information you store on them in Timemaster. 7
5.3 Deleting personal information 7

Version history

30 April 2018 - First issue (Matt Norris)

1. Introduction

1.1 What is GDPR?

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union. It becomes enforceable from 25 May 2018 and replaces the 1995 Data Protection Directive.

1.2 Who does the GDPR affect?

The GDPR not only applies to organisations located within the EU, but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

1.3 What constitutes personal data?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

1.4 Why should it concern you?

Being a Timemaster administrator, you have access to personal data stored within Timemaster. You also control user access rights to this data. So, you play a key role in controlling the visibility of this information, and how and where it's used.

1.5 Document Scope

This document outlines what you need to consider in relation to the information you store within Timemaster so that you comply with the new GDPR legislation.

1.6 Disclaimer

This article is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your business. We encourage you to work with a legally-qualified professional to discuss GDPR, how it applies specifically to your business, and how best to ensure compliance.

2. What personal information is held within Timemaster?

Contact Details

- Staff Name (inc. Title, Initials and Salutation)
- Staff ID
- Home Address
- Home Telephone

Note: The staff member's photograph may also be stored.

Employment Details

- Job Title
- National Insurance No
- Car Registration No
- Payroll No
- Mobile No
- Work Telephone No
- Email
- Outlook Email
- Home Location
- Distance to Office
- Employment Start Date
- Employment End Date
- Notes

Payroll

- Salary level
- Gross Salary
- Net Salary
- Additional Salary
- NI Pension Uplift
- Date of next review

Accounting Interface

- Sage Account Number
- Sales Ledger Nominal for expenses
- Sales Ledger Nominal for time
- Purchase Ledger Nominal for Expenses

Additional Information

- Days Holiday
- Swipe Card Number

Note: Additional personal information may also be stored in staff user fields.

Note: Personal information may be exposed on expense receipts – staff should be encouraged to redact this information from the receipt before uploading it into Timemaster.

3. Informing staff of their GDPR rights

3.1 Auto prompting (Login Message) feature

We've added a new feature that can automatically display a message to all staff when they log in. This message can be used to inform them of their rights and responsibilities in relation to the GDPR legislation.

This is turned **off** by default but can be turned on via;-

Windows application ⇢ Setups ⇢ Control Codes ⇢ Control Parameters ⇢ Staff details tab page ⇢ **Display message on first login**

The message itself can be altered to suit your company's requirements and will then be displayed when users log into the system. The system will record the user's acknowledge to the message in their staff history (Staff ⇢ Staff Audit History).

Note: This new Login Message feature can also be set to auto prompt the user after a set period.

Changes to the wording of the Login Message text will automatically trigger the message to appear the next time users log in, thus enforcing a new acknowledgement from the user.

4. How can staff view their own personal information you store in Timemaster?

4.1 My Details

Staff can view the key personal information you store on them within Timemaster by navigating to;-

Home ⇢ My Details

This is controlled by a new access right;-

Staff Related Functions ⇢ View My Staff Details

Note: This access right is turned **off** by default. However, you can grant this to the **USERS** login group if you want ALL users to have access to this feature.

A more comprehensive list that includes notes etc. can be obtained by using the Crystal Report **Personal_Data_Request Report** (Tm_Personal_Data_Request.rpt).

5. Protecting access to personal data?

5.1 Controlling access to personal data.

Note: You should ensure that the Timemaster 'Admin' user is assigned a strong password as this will reduce the likelihood of unauthorised access to the Timemaster system!

As a Timemaster Administrator, you're probably familiar with the way access rights work within Timemaster; users are assigned one or more login group, each login group contains a range of access rights.

You can check individual user access rights via System Administration ⇢ Log Users. Alternatively, you can run the following reports from with the Admin Reports reports sub category;-

- Login Access Rights report
- Users and Groups Report
- Login Group Membership report

So, you will need to consider restricting users to the following access rights if it is deemed they should not have access to staff personal information; -

Staff Related Functions

- **View My Details** – enables the staff member to view their most pertinent personal data stored in Timemaster.
- **Edit Staff Records** – provides access to much of the staff member's personal information.
- **Show Staff Salaries within Staff Record** – enables users to access the staff member's salary information.
- **Show Hourly Rates within Staff Record** – gives users access to staff hourly rates stored against the Staff Reports.
- **Staff Hourly Rates** – provides access to staff hourly rates from other parts of the system.

Reports

- **Staff Reports** – users with this access right can access reports containing staff personal information*.
- **User Reports** – you may have written a custom Crystal report that reports on staff personal information. It is your responsibility to check these reports and who has access to them.

* If users are granted access to Staff Records, we recommend you consider also implementing the following 'Report Restrictions' access rights.

Report Restrictions

- **Restrict Staff Reports by Line Manager** – limits staff shown on Staff Reports to only staff the user is a line manager of.
- **Restrict Staff Reports by Own Record** – limits staff shown on Staff Reports to the user's own staff record.

Note: Staff may have individual Staff or User reports allocated to their Favourite Reports. It is your responsibility to check which reports have been added to users Favourite Reports.

System Administration

- **Login Users** – provides a mechanism for users to grant themselves additional access rights by adding additional Login Groups to their user record.
- **Login Groups** – provides a means for users to grant themselves additional access rights to their login record.
- **Reset User Passwords** – allows users to reset a different user's password and thus log in as a different user with elevated access rights.
- **Execute SQL Script** – enables users with SQL knowledge to gain access to staff information by querying the staff table.

Also note that users, like yourselves, may have the **System Administrator Privileges** assigned to them. This is an important access right as it over-rules all other access rights and therefore gives users access to ALL Timemaster functions.

When reviewing user access rights, you may also want to consider who is currently an admin user. Admin users are highlighted in the users list - ask yourself "do they really need to be an admin user?"

Note: Please feel free to get in touch with us if you are unsure about any of these concepts.

5.2 Providing details of what personal information you store on them in Timemaster.

A new Crystal Report **Personal Data Request Report** (Tm_Personal_Data_Request.rpt) is now available. This report can be located under the **Staff Reports** sub category and can be used if ex-employees request a report detailing what personal information you hold on them in Timemaster.

Note: Please run System Administration ⇢ Refresh Report Selections and Menus if this is not shown in the reports list!

Note: This report is only accessible by Timemaster System Administrators, or users who have the **Reports** ⇢ **Staff Reports** access right assigned to them.

5.3 Deleting personal information

Employers will have legitimate interests to process and store personal staff data under the GDPR. This business need takes precedence over the individual's right-to-be-forgotten.

Before deleting any personal staff information, you need to consider which information you are required to keep and for how long. Once you have this established this, delete any information you no longer need to keep then issue the Personal data stored in Timemaster report **Personal Data Request Report** (Tm_Personal_Data_Request.rpt) as confirmation.