Time & Attendance, Biometrics, Access/Door Control entry and GDPR

(General Data Protection Regulation)

What does it mean for your business and your customers?

ACTIN TIME LTD
WORKFORCE MANAGEMENT SYSTEMS

Many companies are strengthening their internal & external policies to comply with the new GDPR regulations which come in to effect on 25 May 2018 which replaces an outdated data protection directive from 1995.

ActIn Time Ltd has always taken the Data Protection Act very seriously and has been a registered member since 30th July 2003.

ico.
Information Commissioner's Office

Upholding information rights
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Certificate

Organisation Name:

Actin Time Ltd

Reference number:

ZB056811

Tier:

Tier 1

Start date:

4 May 2021

End date:

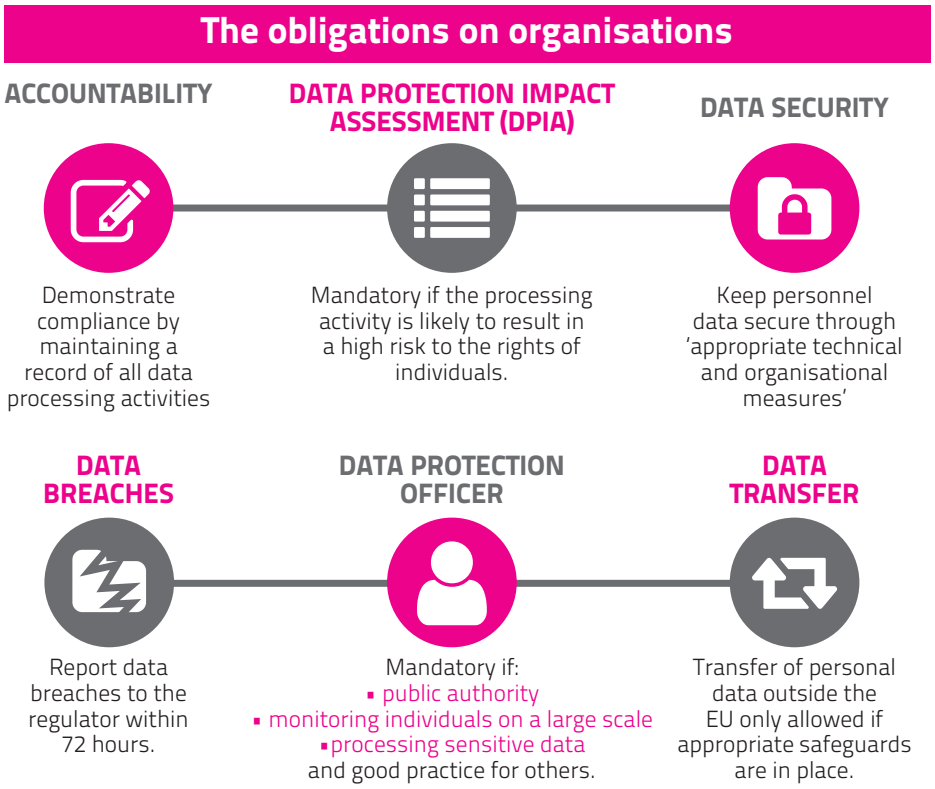
3 May 2023

Data Protection Officer

A lot of focus is aimed at internal & external data processes for employees, making sure 3rd party companies who have access to their data take precautions to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.

However, that standard is quite complex, and in many occasions, very confusing. Fundamentally each company is responsible for its own compliance with GDPR whether it be a paper system or digitally stored data. Let's not forget, most of the GDPR principles have always been standard practice for companies for years, the new legislation is now here to enforce them.

> *"On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?"*



As your supplier we are proud to inform you that we are tackling this on two fronts.

1. General

a. ActIn Time's internal policies and securities updated to increase security for customers data.

b. All existing engineers USB sticks will be replaced with security USB devices to protect customers data in transit i.e. Flash Padlock® 3 Secure USB 3.0 Flash Drive, CORSAIR PADLOCK 3 USB 3.0 flash drive is designed to provide government level security, environmental protection, and an easy to use interface for your most important data. i.e. https://www.corsair.com/uk/en/Unformatted-Capacity/flash-padlock-3-config/p/CMFPLA3B-64GB

c. New secure SFTP servers for data transfer.

d. Databases, spreadsheets, employee lists etc. will be deleted and removed from our servers on a regular basis to comply with the new regulations.

e. FTP sites, engineers general standard USB sticks are no longer to be used. Any printed copies of customer's data will also be destroyed securely.

f. Data will be kept no longer than deemed necessary whilst new installations, upgrades or technical issues are ongoing, after which it will be destroyed.

g. More awareness to our customers on security and encouraged to increase protection for backups or any other programming data.

h. No data to be removed from site unless deemed necessary for technical issues and customers will be advised accordingly.

2. Software

What does this mean for a company using an ActIn Time 2018 workforce management system?

If an employee wants to see all their data, how would you respond and how long would it take? Whatever method of storing data i.e. paper/digital in one system or spread across multiple, the rules are the same for security and safety, these are the considerations companies are facing today.

What next?

Before your installation/upgrade, an ActIn Time technician will discuss your company's GDPR policy with your GDPR data controller.

This meeting will cover two main areas:

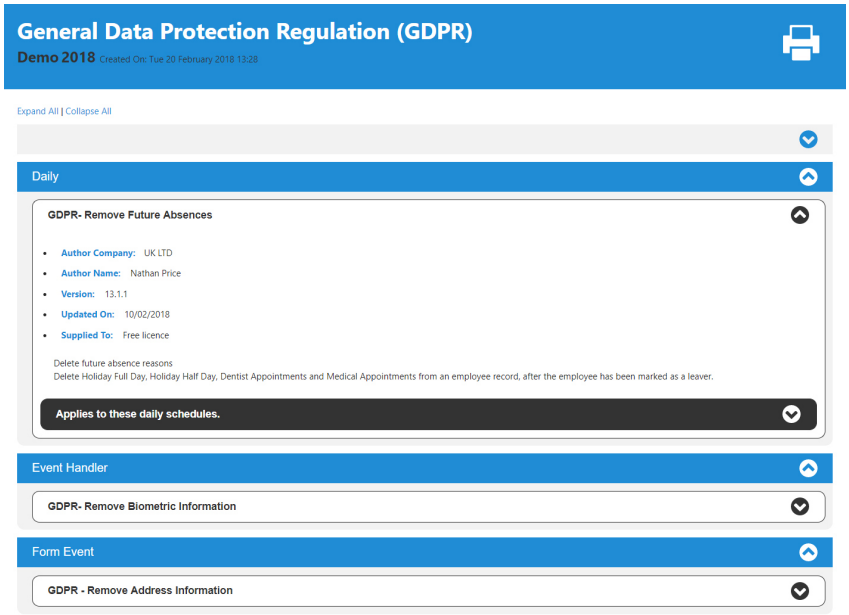
1. The way in which we handle your company data which in turn will impact on the way our support team provides certain types of service e.g. your business may require that we never remove personal data from site. This information must be recorded against your SLA notes to ensure we do not create an environment where a personal data breach could occur.

2. The processing of personal data stored within the ActIn Time application. We will identify any personal information fields within ActIn Time that do not need to be recorded and take steps to ensure that they are hidden. We will also discuss how long certain information needs to be kept by the company for people classed as employed or as a leaver. We will then create/modify the default GDPR housekeeping scripts that will ensure these rules are upheld. Any other specific company requests can be discussed separately because each company may have a different set of GDPR policies they would like us to comply with.

Please note that ActIn Time will never delete any personal data. We think it is much safer that ActIn Time operates within your data controller's policies and highlights data that requires deletion. This will always be completed by your data controller and is fully audited.

Some example GDPR housekeeping scripts:

1. If ActIn Time is not being used as the primary HR system do not allow address information to be recorded.
2. If ActIn Time is not being used as the primary HR system do not allow National Insurance data to be recorded.
3. When an employee leaves the company, remove their biometric data within 24 hours.
4. When an employee leaves the company, remove all records of their future holidays and medical appointments within 24 hours.
5. When an employee leaves the company, delete all passwords to the ActIn Time app', the TWC and the ESS within 24 hours.
6. When an employee has left the company after the statutory period, remove all attendance, absence information and personal data.



Biometric Data

Importantly, under the GDPR, biometric data is classified for the first time as a 'special category' of personal data, meaning that it cannot be processed by employers unless it satisfies one of the additional conditions that permit the processing of special category personal data in specific and limited circumstances. These are: obtaining 'explicit consent' (although obtaining valid consent in an employment context will be much more difficult under the GDPR and requires further consideration), or where it is necessary for the purpose of carrying out obligations or exercising specific rights under employment and social security law or under a collective agreement.

The GDPR also introduces a requirement to perform a privacy impact assessment in relation to processing, which is likely to be high risk to the rights of the individual, and specifically makes privacy impact assessments mandatory in relation to large-scale processing of special category personal data. In certain circumstances it may also be necessary to consult the Information Commissioner's Office (the UK data protection regulator) before starting any high-risk processing.

Compliance with the GDPR should be taken into consideration at all stages of implementing a biometric system and the employer should seek specialist legal advice early on.

It is important to understand that the manufacturer or supplier is not responsible for data protection inside, let's say, a fingerprint, face or hand Time Attendance terminal. It is how and where one saves the data that matters. Typically when employees enrol at Biometric device, the template saved into the device is not the whole, let's say finger for example purposes. When templates are created they are made up of a number of only minutiae ridges & points taken from the finger and not the complete finger scan. This is then securely saved away inside the device and sent to the software database for backup or template movement to other devices. An example of the data string for each template saved away is as follows: -

D8EDE650A6CD065E5E03DC99CA8C758E5EFC2E496CEFF1E4A77B752B3E8DCFDBCBC968ABDA77D89E1FF83DA8C87D4091F7AA13F54DC53223B0B7910FBA710A6FF8B8E9ED4D6D33F8207741A47643D21B9A346E49AD0388748E8B6B0307209E44B034BEC5EB403B43949FDC46630A043A0E9C0CE5E9334BF375FA39955F52E3BF87EE0A1CBF59F73C3C061FC171C4E1D41B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06CF97C1B2DC9EBAF0D5F602A64FF47F06C

5 Popular questions being asked as follows:-

1. Can we delete archive employees historical data?

Yes, you can delete employees from the personnel screen within ActIn Time manually. This will delete the complete employee record from the database including the biometric template for the clocking device stored in the database. You should use the DELETE option for the employee with extreme care because it is irreversible and you may need/want to keep certain information for historical records which is governed by law for 7 years for limited companies. Alternatively you could delete certain records within the employee record that is no longer necessary to keep on record, i.e. Next of kin, training, job specification, national insurance no, passport no, address, medical, future absences etc. Warning – if you are using the software for Job Costing, this will delete all records worked for this employee on historical jobs which will affect ALL the job totals. It is not advisable to DELETE employee's entire record if this module is being used.

2. Can we delete old data to help speed up the software?

Upgrading to the latest version and carrying out a FREE System Health Check will certainly help the areas you are trying to address and we can advise on the way forward. This will pinpoint any hotspot areas on potential system speeds, SQL database limit reached, database shrinking required, network stability/reliability etc.

3. How will ActIn Time 2018 (GDPR Tools) help us comply?

ActIn Time 2018 (incl. GDPR Tools) has now been released which includes built in tools to help customers specify their own GDPR criteria with automatic pop up alerts for users on their 'To Do List". Specific company GDPR policy rules can be applied as a global setting for specific fields within the database that apply to each company i.e. when someone leaves, an action should take place after 'x" amount of days to remove their personnel, biometric template, future absences, contact details etc. type of records. The upgrade is FREE (if covered under your service agreement) to 2018 but the GDPR tools are an optional feature that has to be setup with a GDPR project consultation meeting, plus end user training.

Unfortunately due to these overheads/conditions and the solution having to be tailored to each client, we are unable to carry out free upgrades to customers wishing to utilise the new GDPR module because this requires additional setup time.

Each customer will have to undergo an ActIn Time GDPR audit on how they want the software to interact with their own company GDPR rules. It is important at this stage to point out that although there are a series of default GDPR scripts that have already been written which can slightly tweaked per client, that we also have the ability to customise additional scripts on a per client basis should the defaults not quite suit.

The GDPR tools will become more useful as your system grows with your employee data and features you intend to use.

4. What does a GDPR consultation & configuration audit include?

- GDPR project build & ActIn Time audit consultation.
- Customisation discussion for your own company rules.
- Setup for the default GDPR script.
- GDPR Feature awareness training.
- System Health Check for historic data.
- Data cleansing (deletion & speed issues).Security – Password & Permission review.
- Email password recovery for all users.

5. Can ActIn Time Ltd access our ActIn Time software or Database?

No, the ActIn Time System is installed on your server/pc, with security and permissions that are governed by you. The system runs from a secure SQL database for which your IT are responsible for keeping the passwords secure. We can only access your database as and when you allow us to for support.

What's next?

Basic steps we would advise, is to re-evaluate any device or software passwords and to make sure all default passwords are changed at point of installation or upgrade. Any user emails being used for the ESS/TWC portal should use the NEW method of email security where the employee controls/sets up their own password which is then stored in the database in a encrypted format.

Over the coming weeks we will be continually looking to update our company policies and listen to our customers' requests on what they feel would be beneficial.

We hope that this may help answer some doubts regarding the GDPR. Should there be any further questions that you have, please do not hesitate to contact us.

We promise that we will do our best to assist you in any way we can.

ActIn Time Ltd would like to thank you for your business over the years and express to you our full commitment to ensuring that this new regulation become part of our day to day business, and rather than hinder, we are confident it will have a positive effect on the solutions we offer.