

Summary of Service

The Data Protection Act (DPA) was put in place to help protect people's personal data. It aims to ensure that people know where their data is held, what it is used for and who it is shared with. It also makes sure that an organisation treats people's data correctly and has systems in place for managing the information.

Details of Service

The Data Protection Act is a law that was introduced in order to comply with the European Directive 1995 and replaces the Data Protection Act 1984. It also amends or partially repeals other statutes.

The new Act is the legal framework within which all organisations who are controllers of personal data must operate. It covers all data held about an individual (data subject) in both manual and computerised files.

Personal data is any information about an individual from which the individual can be identified, i.e. name, address, date of birth, photograph, video image, Payroll Number, etc, Personal information also includes any written opinions about the individual.

This document is designed to assist our construction clients with their Data Protection Act Policies and to outline how SiteRec complies.

Data Protection - eight principles

Personal data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in line with the data subject's (individual) rights
7. Secure
8. Not transferred to countries outside of the EU without adequate protection

Principle 1 Fairly and Lawfully Processed

Fair - you must inform users of SiteRec about the reasons why their information is used. This could be for several reasons: you wish to protect their pay by ensuring that accurate attendance information is collected, you wish to protect them in the event of a roll call (if they have clocked on for work or if they have activated a turnstile using their biometric,

they should be on your site. If there is an emergency a report can be easily obtained of all people that are on your site).

Lawfully – as a company you should ensure that you are not working outside of your powers.

- Your workers must have given their consent. (This does not have to be in writing)
- Contracts - the use of SiteRec might be necessary: -
 - a) to carry out a contract to which you have signed up
 - b) at your request with a view to entering into a contract
- Vital interests -the use is necessary to protect your vital interests.
- Legitimate interests - the use is necessary for legitimate interests pursued by your company (this could be to streamline your payroll processes, to fit in with your environmental policy and cut down on the use of paper or any other purpose)

Principle 2 Processed for limited purposes

Information must not be used in any way incompatible with the purposes it was originally collected for. E.g. information collected for time and attendance cannot be used for identification purposes without gaining further consent from your employee. SiteRec is designed for verification only. Ie when a person has been added to SiteRec, they input a PIN number or present a card. This tells SiteRec to go to a single database record and to compare the person with that record only. SiteRec is not able to perform any other biometric task (ie SiteRec is not able to find out IF the person is known, only to confirm if they are who they report to be).

Principle 3 Adequate relevant and not excessive

You must collect enough information to do the task or provide the service but must ensure that what you collect is needed and that you are not collecting information “just in case”. SiteRec only has three ‘compulsory fields’ which are the first name, surname and their PIN/card number. By itself this information is useless. Templates must also therefore be added to the person’s record. Aurora construction customers have used SiteRec since the late 1990’s and the addition of fields for further information has only arisen as a result of companies internal processes. The collection for example of information about next of kin or home address may not be relevant to all users of SiteRec. This is why these fields are not compulsory.

Principle 4 Accurate

As a company you must take care of the information held and make sure that it is kept accurate. SiteRec has built in ‘tools’ to ensure that the person’s templates are up to date. The frequency is configurable but SiteRec customers tend to keep with the software defaults (every 10 successful clocking events or every 2 weeks whichever is the sooner). This means that when a person has successfully clocked in for work or gained access via a turnstile controlled with SiteRec, the software analyses the face and compares it against the stored templates. If the face scores higher, the worst template is removed and

replaced with the new one. SiteRec therefore automatically ensures that data is up-to-date. Other data that is deemed necessary by the company should be checked on a regular basis to comply thoroughly with this point of the Data Protection Act. As SiteRec can be moved from site to site the data can be checked as each new employee is given their site induction at each new site.

Principle 5 Not kept for longer than is necessary

The length of time that information should be kept is not set out under the Data Protection Act. When there is no such guidance the length of time to keep information is set by the company. SiteRec however does enable templates to be deleted at the touch of a button. This does not result in transaction history being deleted (you might need to keep this information for costing purposes or to ensure that subsequent pay is accurate). SiteRec does enable archiving of data on a regular basis and when a new site starts, a fresh database is created.

Principle 6 Processed in line with the data subject's (individual) rights

Your employees have the right to ask for any information held on them. SiteRec has the ability to access just one database record for any amendments necessary. You can therefore show your employee information held JUST ON THEM. This protects the DPA rights of the remainder of your employees.

Of course outside of this, you must ensure that any data held in SiteRec is not sold on to a 3rd party (for direct marketing as an example).

Principle 7 Security

As a company you must ensure that the data held within SiteRec is secure. This means that your staff are trained on how to use the software and that only authorised people can access it. The DPA states that data must be protected against:

- Unauthorised and unlawful use
- Accidental loss

SiteRec has a password protection system. There are three levels of password at site level. When SiteRec is installed, one person only from your company is given the necessary level of password to add, amend and use SiteRec. It is this person that your office normally gives Aurora as the site contact.

SiteRec has automated back-up routines. In the event of a 'one booth system' being purchased, Aurora provides an additional external hard-drive as standard. It is to and from this hard drive that data is backed up. In the event of a two booth (or more) system being purchased, the back-up routines are to and from the provided PCs.

Principle 8 Not transferred to countries outside of the EU without adequate protection

You must not transfer personal information to countries outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects. SiteRec is used in the UK on a per site basis. However there is one element of SiteRec called 'web reporting'. By placing data on the Internet, it might be perceived as being transferred to every country in the world. Not so. The web reports are only given to certain fixed IP addresses. And even then, a password system is in place.

Aurora IT professionals are available at any time to give further advice about network and IT security.

Some useful information

The UK Government is pro biometric use and there are schemes in place to include biometrics in passports, National ID cards and driving licences.

The Identity and Passport Service (IPS) was established as an Executive Agency of the Home Office on 1st April 2006. The Agency is to provide passport services and in the future, as part of the National Identity Scheme, ID cards for British and Irish nationals and foreign nationals resident in the UK which contain biometrics.

Source: the Home Office website on the use of biometrics for identity cards www.identitycards.gov.uk

What's the benefit of using biometrics?

Because your biometrics are unique to you, they are the strongest way to 'seal' your identity details as held in the National Identity Register (NIR) to you. The most secure identity check would involve confirming, not just that you have a valid identity card, but that the card and the record that matches it belong to you. This is a far more secure way of identifying yourself than using a personal identification number PIN or password, which could be stolen or copied.

The use of biometric data offers you the greatest protection from identity fraud. A criminal may steal your card, but your unique biometric data cannot be taken from you. Anyone trying to make a major financial transaction, for example, would have their biometrics data checked against those held in the NIR. If they were not the registered cardholder this check would fail.

Biometrics are also the best way to prevent criminals from registering for more than one identity card - they could supply a false name and forged documents, but their biometrics would be picked up