EU GENERAL DATA PROTECTION POLICY (GDPR)

Data Protection Act 2018

The EU'S General Data Protection Regulation (GDPR) will come into force in May 2018. The Data Protection Bill (the Bill), replaces the previous Data Protection Act of 1998 and forms part of the UK's new regulatory framework, the GDPR. It aims to balance the entitlement of organisations to collect store and manage various types of personal data, with the privacy rights of the individual about whom the data is held. It introduced the principles of good practice, a registration system, an independent supervisory authority and the data subject's right to access personal data held about him or her and have inaccuracies corrected or removed.
The Act covers manual and computerised records and processing data related to identifiable living individuals. It gives individuals certain rights, and requires decision-makers to be open about processing and to comply with the data protection principles.

GDPR's accountability principle requires organisations to be able to show how they comply with the GDPR principles; by having effective policies and procedures in place. Information is to be provided in a concise and easy to understand, clear language.

The GDPR enforce the following rights for individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object and
- The right not to be subject to automated decision making, including profiling

Employers' Duties

Employers have a duty to:

1. Give accurate information if they decide to supply a reference for an employee/ex-employee
2. Only request personal data from employees that is relevant and not excessive in relation to the purpose it was requested for not retain personal data for longer than is necessary
3. Update personal data where necessary to ensure the information is accurate, ensuring records of processing activities is maintained.
4. Put in place technical and organisational measures against unauthorised access
5. Arrange safeguards to prevent the accidental loss, destruction or damage of data
6. Not process data without the employees' explicit consent, except where there is a legal obligation on the employer to do so or a number of other exceptions apply
7. Not process sensitive personal data without first satisfying the legal requirements
8. Request permission from the employees when obtaining third party records, e.g. medical records,
9. Supply personal data to an employee on request.
10. Where information has been shared with another organisation and it is later found to be incorrect the relevant organisation must be notified of the inaccuracies so that they can update their records.
11. Communicating privacy information; the employer will need to explain their lawful basis for processing the data they request, hold or share on an employee.
12. Point nine (above) is also relevant for the data retention periods; it has to be justified on a lawful basis.
13. Identify and document your lawful basis for your processing activities in order to comply with GDPR's 'accountability' requirements.

Subject access requests:

- In most cases you will not be able to charge for complying with a request.
- You will have a one month to reply to an individual request.
- You can charge or refuse requests which are manifestly unfounded or excessive.
- If you refuse a request you must tell the individual why and that they have a right to complain to the supervisory authority and to a judicial remedy. You must do it without undue delay, at the latest, within one month.
- Ensure there are processes in place to effectively detect report and investigate a personal data breach. In particular where it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage.
- If there is a breach in relation to the rights or freedom of the individual you must also notify them directly.

Employees' Duties

Employees have a duty to:

1. Not provide information that is misleading or inaccurate. Only request to see information that is personal data.
2. Not Sending emails to colleagues that amount to harassment or bullying that could lead to employment tribunal claims.
3. Not entering into contracts on the internet on behalf of the employer without authority.
4. Infecting the employer's system with viruses.
5. Hacking.
6. Breaching a third party's intellectual property rights, e.g. by copying material from the internet.
7. Damaging the Company's reputation, e.g. by tweeting that the Company's products are no good or by being rude to customers on the telephone.
8. Divulging company confidential information to third parties without the permission of the managing director.
9. The employee has a right to complain to the ICO (https://ico.org.uk/for-organisations/) if they think there is a problem with the way the employer is handling their data.
10. Employees must opt-in whenever data is collected and there must be clear privacy notices. These notices must be clear and transparent and consent can be withdrawn at any time.

Note:

The employee has the right to request erasures which includes all data including web records being permanently deleted.

Processing of Sensitive Personal data.

Sensitive personal data relates to:

- Ethnic or racial origin
- Political opinions
- Religious or other similar beliefs
- Physical or mental health
- Sexual life
- The commission or alleged commission of any offence and any related proceedings or sentence
- Online identifiers
- Location data
- Genetic data

Processing of sensitive data is only permitted where:

- The individual has given his or her explicit consent to the processing
- It is necessary to protect the vital interests of the individual or another person, in cases where consent either cannot be given, has been unreasonably refused or where the employer cannot reasonably be expected to get consent
- The data has already been made public by the subject
- It is necessary in connection with actual or prospective legal proceedings
- It is necessary for the administration of justice
- It is necessary for medical purposes and is carried out by someone with a duty of confidentiality
- It is necessary for equal-opportunity monitoring and the data relates to racial or ethnic origin.
- Employees have a right to have their data deleted where the company use consent as their lawful basis for processing.

Consent has to be of GDPR standard, which includes:

- Specific
- Clear
- Prominent
- Opt – In
- Properly documented
- Easily withdrawn.

The data Protection Codes state what employers need to check . They cover how employees should be treated relating to:

- Recruitment and selection
- Employment records
- Employee monitoring
- Medical records.

Applications
When dealing with job applications, including curriculum vitae and unsolicited applications, employers should:

- State who will receive information and how it will be used
- Only obtain relevant/necessary personal data
- Only seek information about criminal convictions if justified by the role
- Tell candidates what checks will be undertaken, e.g. references, qualifications and health checks
- In the case of sensitive data, ensure that at least one sensitive data condition is satisfied
- Provide confidential means of sending/receiving applications.

Verifying Applicants' Claims
When verifying candidates' claims through references, verifying qualifications and financial information, employers should:

- Explain what checks they intend to make
- Obtain consent before obtaining third party records
- Seek candidate's comments if discrepancies show up
- Only seek verification on a need-to-know basis.

Shortlisting
When shortlisting applicants, employers should:

- Use personal data consistently
- Tell candidates if only automated shortlisting is used and allow them to comment on results
- Ensure psychological testers are fully trained.

Following interviews of candidates, the employer should ensure that any personal data retained afterwards are necessary for justifying the selection decision.

Pre-employment Vetting
Employers should take care when carrying out pre-employment checks as it may seem intrusive. It is advisable to carry out checks only where:

- Employer, clients or customers may be at significant risk and there is no alternative
- A candidate has been offered the position
- Candidates have been informed that the checks will be carried out
- Information sought has been specified
- Reliable sources have been used
- Exceptionally, the family needs to be approached
- The person's consent to approaching third parties has been obtained
- Medical checks are required.

Retention of Recruitment Records
Other than for the successful applicant, recruitment records should not be retained any longer than is necessary for making an appointment and responding to any challenges to that appointment. If records are retained because applicants might be considered for other vacancies that arise in the future, applicants should be advised of this and given the opportunity to say no. A period, from first application to destroying of data, of twelve months is seen by the company as being appropriate.

Employee Records
Personal records need to be held for the purpose of staff administration. However, the risk to employees if decisions are taken or opinions formed on the basis of inaccurate or inadequate records are obvious as are the risks if records are not kept securely.
Collection of Information:
Do not seek personal information from employees that are irrelevant or excessive to the employment relationship.
Maintaining Records:
These should be accurate and up to date. Out of date information or information that is no longer required should be deleted.

Sickness Records:
Sickness records are almost certain to include sensitive data and should be treated as such.

Security:
Particular care should be taken when transmitting employee information by e-mail. Under no circumstances should employee information be sent by fax. Accessing, disclosing or otherwise using employee records without authority may be treated as a serious disciplinary offence and such conduct may constitute a criminal offence.

Training Records:
Records can be held on file that covers both statutory and none statutory training data. However the company, because of its diverse client base, is required under qualifying criteria to maintain training records that are compliant to a particular regime. These records must also be available to inspection to not only client organisations, but individuals as well. No sensitive personal data must be held within the training records if these are held outside of the company designated process.

Access to Employee Data

Employees are allowed to have access to all personal data about them held under the General Data Protection Regulation Act 2018. This Act requires the Company to respond to requests for access to personal data within 30 days.

The Data Protection Act 1998 gives employees the right to have access to their personal data at reasonable intervals, which the Company deems to be every 6 months.

Should employees request access to their personal data at any other time, the request must be addressed to their line Director. Subject access requests are free of charge and must be actioned within 30 days.

The request will be judged in the light of the nature of the personal data and the frequency with which they are updated.
The employee will then be informed whether or not the request is to be granted. If it is, the information will be provided within 30 days of the date of the request.

In the event of a disagreement between an employee and the Company regarding personal data, the matter should be taken up under the Company's formal grievance procedure.

Any person who has material or non-material damage is entitled to claim compensation.

All employees, ex-employees and job applicants have the right to request the employer for access to any specified personal data held about them.

Personal data includes details of:

- Sickness
- Discipline
- Training
- Appraisal
- E-mails
- Word-processed documents
- Audit trails
- Information on personnel files
- Interview notes
- Medical Testing

Types of Testing:
Medical testing includes drug testing, alcohol testing, HIV/AIDS testing and genetic testing as well as more general medical testing.

Testing Employees:
Testing should only occur where it is part of a health and safety programme operating in the interests of employees or it is a necessary and proportionate measure to:

- Prevent a significant risk to the health and safety of the employee or others;
- Determine the employee's fitness for continued employment;
- To determine the employee's entitlement to health related benefits e.g. sick pay.

Testing Potential Employees:
Testing of potential employees should only occur if they are considered suitable for employment on all other grounds and testing is necessary to:

- Determine whether the potential employee is fit for the particular employment;
- Meet any legal requirements for testing;
- Determine whether the potential employee is eligible to join a pension or insurance scheme.

Retaining Records
This section addresses the general retention of records of employees and former employees. Information will not be kept for longer than is necessary but equally it will not be discarded when doing so would render the record inadequate. Where specific legal provisions require the retention of employment records for a set period then this is the minimum time for which they will be retained. Information will not be retained simply on the basis that it might come in useful one day. Records that are no longer required will be properly and securely disposed of.

Retention period
In the absence of a specific business case supporting longer retention periods the following will be used as a guideline:

Type of record	
Application form	Duration of employment (1 Year if not employed)
References received	1 year
Payroll and tax information	7 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years Liability Insurance requirement
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given	5 years from reference/end of employment
Records relating to accident or injury at work	3 years

Computer Security
The Company regards the integrity of its computer system as central to the success of the Company. Its policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected.

Procedure
Overall computer security is the responsibility of the Office Manager; line managers are responsible for security within their own departments.

In the case of a personal data breach, data controllers (all employees who have access to personal data both customer and employee) shall without undue delay, and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority unless the personal data breach is "unlikely to result in a risk for the rights and freedoms of individuals".

If a notification is not made within 72 hours of the data breach, the data controller must give a 'reasoned justification' explaining the reason for the delay

1. On induction and where relevant employees will be given copies of the Company policy, e-mail and Internet Access where applicable and will receive written instructions on security procedures.
2. Computer use at every level will emphasise the importance of security.
3. Staff will receive a briefing on the implications of the EU'S General Data Protection Regulation (GDPR) formerly Data Protection Act 1998 and the Computer Misuse Act 1990.
4. Supervisors are responsible for ensuring that basic procedures are followed.
5. Procedures may be bypassed only with the consent of a Director.
6. Employees of all grades are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Levels of access will be decided by line managers.
7. Employees may access the Internet but access to certain sites may be restricted.
8. All incoming emails will be monitored and scanned for viruses before being released to the recipient via the IT support consultant / software.
9. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the Data Protection Act.
10. Passwords must be used at all times and changed regularly. Employees should not select obvious passwords. Passwords must be kept confidential. Employees must not give their passwords to other members of staff or to any person outside the Company. The only exception is when authorised by a Director and/or the Company approved IT consultant.
11. All the Company's software must be formally authorised by the Company approved IT consultant.
12. Regular checks will be made for viruses by the Company approved IT consultant.
13. No external software may be used without authorisation by both the Managing Director and the Company approved IT consultant.
14. The safekeeping of CDs and DVDs sent from external sources is the responsibility of the person to whom it was sent. All such CDs and DVDs must be checked for viruses by the Company approved IT consultant before use. CDs and DVDs generated internally must be kept in a secure place.

Misuse of computers is a serious disciplinary offence. The following are examples of misuse:

- Fraud and theft
- System sabotage
- Introduction of viruses, etc.
- Using unauthorised software
- Obtaining unauthorised access
- Breaches of the Data Protection Act
- Sending abusive, rude or defamatory messages via email
- Attempting to access prohibited sites on the internet
- Hacking
- Breach of the Company's security procedures.

This list is not exhaustive. Depending on the circumstances of each case, misuse of the computer system may be considered gross misconduct. Please refer to the disciplinary rules and procedures. Misuse amounting to criminal conduct may be reported to the police.

E P Industries reserve the right to monitor Company e-mails sent and received by Company e-mail addresses under the telecommunication (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Computer security will be regularly reviewed by the Company IT consultant.
All breaches of computer security must be referred to the Managing Director. Where a criminal offence may have been committed the M.D. will decide whether to involve the police.

Any member of staff who suspects that a fellow employee (of whatever seniority) is abusing the computer system may speak in confidence to their line manager or supervisor.

Signed: **EDWIN PILSWORTH**

Managing Director

Date: **13/02/2018**

Policy read and understood by employee: NAME _____

POSISTION _____

DATE _____