What is the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation is the new governing legislation for collecting and processing personal data in the EU.

It comes into effect on 25 May 2018. The Government has also published the Data Protection Bill, which will supplement the GDPR, replacing the Data Protection Act 1998.

The GDPR requires that personal data be processed according to many of the same principles as under the current Data Protection Act 1998. However, the GDPR has new requirements:

- The use of consent as a justification for processing data is restricted;
- Data processing activities must be documented to demonstrate compliance;
- Organisations must have measures in place for data protection such as policies and practices; and
- More information must be provided to employees and job applicants on the reasons and legal grounds for collecting their data, and their rights in relation to their personal data.

The GDPR also creates a new enforcement system, with significantly higher maximum penalties than under the Data Protection Act 1998. In particular, breach of the GDPR in some circumstances can lead to a maximum fine of €20 million or 4% of an undertaking's worldwide annual turnover, whichever is higher.

What is personal data under the GDPR?

The General Data Protection Regulation defines personal data as "any information relating to an identified or identifiable natural person". It covers data from which someone can be identified directly or indirectly, in particular by reference to:

- an identifier such as a name, an identification number, location data or an online identifier (such as an IP address); or
- factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The GDPR covers personal data that is stored in a manual filing system if it is accessible according to specific criteria, for example where it is ordered chronologically or alphabetically.

How does the Act affect recruitment and selection?

Because we collect and use information about people as part of our recruitment and selection process, the Data Protection Act applies. For example, we obtain information about people by asking them to complete an application form.

The Act does not prevent you recruiting staff effectively. What it does is help strike a balance between our need for information as an employer, and an applicant’s right to respect for their private life.

The Act requires openness, so applicants should be aware of what information about them is being collected and what it will be used for.

If I want to collect or use information about job applicants, what must I do?

Ensure that when placing an advert the Council is clearly identified – people should know who they are applying to.

Use the information you collect for recruitment and selection only.

Data protection rules apply to recruitment and selection and personal data must be handled with respect.

Application forms are designed to ensure we collect only the data we need for recruitment and selection processes. It is a breach of data protection rules to collect irrelevant or excessive personal information.

Do not collect information from all applicants that is only required from the appointee, e.g. banking details.

Keep the personal information you obtain secure – it should not be disclosed to another organisation.

Only ask for information about criminal convictions if this is justified by the type of job you are recruiting for. Don't ask for 'spent' convictions unless the job is covered by the Exceptions Order to the Rehabilitation of Offenders Act 1974.

If you are going to verify the information a person provides, ensure they know how this will be done and what information will be checked.

If you need to verify criminal conviction information, only do this by getting a 'disclosure' about someone from the CRB. Advice on this can be obtained through the SSC.

Only keep information obtained through a recruitment exercise for as long as there is a clear business need for it. Details regarding unsuccessful applicant must be destroyed six months after an appointment is made. Details of the successful applicant should be retained on the employee's personal file.

Do job applicants have the right to see notes made on them at interview?

Yes, job applicants have the right to see interview notes if the notes are either transferred to computer or form part of a "relevant filing system". The General Data Protection Regulation gives job applicants and other data subjects the right to request copies of personal data that an employer holds about them. The GDPR covers personal data put on paper and held in a structured filing system, as well as computerised personal data. For a manual system to be covered, the data must be accessible according to specific criteria. There must be some sort of system to guide a searcher to where specific information about a named job applicant can be readily found. For example, a set of interview notes filed by name in alphabetical order, or chronologically, is likely to be covered by the GDPR.

Recruiting managers must retain interview notes and application forms for 6 months after the interview date, following which the information should be destroyed. Information regarding the successful applicant will of course be retained on the employee's personal file.

Where an unsuccessful job applicant asks for details of why he or she was not offered the job is the employer obliged to disclose those details?

There is no duty in law for an employer to inform an unsuccessful job applicant why he or she was not selected for the post applied for, even if the applicant makes such a request. However the Council does provide feedback on this in order to be helpful.

Job applicants do, however, have the right under the General Data Protection Regulation to submit a request for access to any information held about them by the employer, provided that the information is held either in a structured manual filing system or on computer. This is

known as a subject access request. On receipt of a valid subject access request, the employer must give the applicant a copy of all the personal data it holds about him or her (with the exception of documents that, if disclosed, would reveal personal information about another person). It follows that if there is written documentation about the reason for not offering the individual the job on file, a copy of that document would have to be disclosed to the individual. There is, however, no duty under the GDPR to disclose information that is not recorded, i.e. there is no duty to create documents for that purpose.

Can an employer ask a prospective employee to fill in a medical questionnaire?

Yes, but only after the individual has been made a job offer and only if it complies with data protection requirements. The Equality Act 2010 prohibits employers from asking job applicants questions about their health before offering them employment (with some exceptions).

Requiring a prospective employee to complete a medical questionnaire after making them an offer of employment requires a legal basis under the General Data Protection Regulation, as this amounts to processing their personal data. The legal basis being that processing is necessary to establish an employee's fitness to do the particular work, to comply with health and safety obligations.

Will employers be able to gather and analyse information for equality monitoring purposes under the GDPR?

Under the General Data Protection Regulation (GDPR), employers are able to gather and analyse information about employees for equality monitoring purposes, provided that they have a legal basis for the processing and, where applicable, the rules relating to processing special categories of personal data are met.

Data that employers gather for the purpose of monitoring equal opportunities will often fall within the special categories of data under the GDPR, i.e. where it relates to employees' racial or ethnic origin, religious or philosophical beliefs, health or sexual orientation. The Data Protection Bill, which supplements the provisions of the GDPR, includes a limited provision that specifically allows these types of special category data to be processed for the purpose of monitoring equality of opportunity or treatment between different groups. An employee can require the employer to stop processing his or her data for that purpose by giving the employer written notice. The employer can rely on this provision if it has an appropriate policy document in place, setting out the safeguards it has implemented for processing special category data and its policies on for how long the data will be retained.

Derbyshire County Council does process data in relation to the above: in some cases we have a legal obligation to do so, and where there is no legal obligation, the data provided by individuals is optional. All reporting is carried out on an anonymised basis.

What are an employer's obligations under the General Data Protection Regulation (GDPR) in relation to the processing of sensitive personal data?

The General Data Protection Regulation (GDPR) uses the phrase "special categories of personal data" to refer to what is known as "sensitive personal data" under the current regime. The special categories of personal data under the GDPR are:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- genetic data and biometric data for the purpose of uniquely identifying an individual; and

- data concerning health, sex life or sexual orientation.

The processing of special categories of personal data is prohibited unless one of the specific grounds set out in the GDPR applies.

The Council collects and monitors this information as under the Equality Act 2010, we are obliged to publish equality information in order to demonstrate compliance with the general public sector equality duty.

Will there be changes to the rules on obtaining consent to process personal data under the General Data Protection Regulation?

Yes, the General Data Protection Regulation (2016/679 EU) (GDPR) significantly restricts the use of consent as a justification for processing employee personal data.

Under the GDPR, consent must be freely given, specific, informed and unambiguous. It must be given by a statement or clear affirmative action. If consent is given through a written declaration, the request for consent must be clearly distinguishable from other matters and easy to understand. The individual has the right to withdraw his or her consent at any time.

The new requirements mean that generic consents are not a valid legal basis to justify processing employee personal data.

The Council is therefore relying on other legal bases to process personal data. See below.

Other than consent, what legal grounds will there be for processing personal data under the General Data Protection Regulation (GDPR)?

Article 6 of the General Data Protection Regulation states that processing of personal data will be lawful only if at least one of the following conditions applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the data controller is subject;
- processing is necessary to protect the vital interests of the data subject or of another person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (this condition does not apply to processing carried out by public authorities in the performance of their tasks).

It is difficult to rely on consent in order to process employment data, as clearly, the imbalance of power in the employment relationship means that consent cannot be freely given. Therefore the Council is relying other bases for processing employee data. For example, the processing of personal data by the employer for the purposes of paying the employee is necessary for the performance of the employment contract, and the processing of data about absence for the purposes of paying statutory sick pay is required for compliance with a legal obligation.

Do employers need to amend employees' contracts to comply with the General Data Protection Regulation (GDPR)?

No, it will not be necessary for employers to amend the contracts of existing employees to comply with the General Data Protection Regulation (GDPR). However, we will be issuing a new privacy notice providing information on the processing of employee's personal data.

This will include the purposes for which we process employee's personal data, the legal basis for the processing, information about the retention period and information about the employee's rights as a data subject.

In a TUPE situation is the transferor required to obtain its employees' consent before passing on information about them to the transferee?

No, the transferor is not required to obtain its employees' consent to disclose information about them in the context of a TUPE transfer, although it must ensure that it has a legal basis for passing on the information under the General Data Protection Regulation.

Under the Transfer of Undertakings (Protection of Employment) Regulations 2006, the transferor has a legal obligation to disclose certain "employee liability information" to the transferee prior to completion of the transfer, including the identity of the transferring employees. As there is a legal obligation to provide this information, data protection rules will not prevent the employer passing it on without anonymisation.

To the extent that the transferor provides information over and above the employee liability information, that is not anonymised, it must ensure that it has an alternative legal basis under the GDPR to process the data. The most relevant basis in this context is likely to be that processing is necessary for the purposes of the legitimate interests pursued by the data controller (in this case the transferor) or by a third party (the transferee). The transferor should obtain formal assurances from the prospective transferee with regard to the use and safekeeping of the information and its return or destruction if the transfer does not proceed.

The employer should provide the employees with a privacy notice informing them that it is transferring their personal data to the transferee (unless the data is anonymised).

Must an employer always obtain an individual's consent before providing a reference for him or her?

Providing a reference is likely to involve processing personal data under the General Data Protection Regulation. Therefore, the employer must ensure that it has a legal basis for processing data. In relation to a reference, the most likely condition to apply is that the individual has consented to the data being processed.

The Information Commissioner's Data protection employment practices code recommends that employers have a policy on giving references that includes a requirement that "all those giving corporate references must be satisfied that the worker wishes the reference to be provided". While the code relates to the Data Protection Act 1998, rather than the GDPR regime, it remains useful for employers, pending updated guidance from the Information Commissioner. The code also recommends that, when an employee leaves the organisation, the employer should keep a record on file of whether or not the employee wishes the employer to provide references on him or her. For example, the employer could ask the employee this question at an exit interview, or it could be included on an exit questionnaire.

If there is any doubt about whether or not the individual has given consent, they should be contacted to check that he or she wishes the reference to be provided, and a note made of their verbal consent.

If an employee asks for a copy of his or her "personnel file" is the employer obliged to supply all the information held on the employee?

Under the General Data Protection Regulation, an individual is entitled to submit a request for access to any personal data that the employer holds about him or her, i.e. any information from which he or she can be identified, directly or indirectly. The GDPR covers personal data held on a structured manual filing system as well as computerised data. The employer must comply with such a request by providing the individual with a copy of the personal data requested.

There are some exceptions to an individual's right of access to personal data. One exception to the employer's duty to disclose personal data is where the information requested is for the purpose of management forecasting or management planning, and where disclosure could prejudice the employer's interests. The other main exception is where disclosure of the information would reveal personal information about a third party who can be identified from the information. In this case, the employer may not automatically refuse to disclose the information. Instead, it should seek either to redact the relevant documents in order to conceal the identity of the third party or, if this is not possible, to seek his or her consent to the disclosure of the information. The employer should also disclose the data if it would be reasonable in all the circumstances to do so without the consent of the third party. What is reasonable will depend on the duty of confidentiality owed to the third party, any steps that the employer has taken to seek his or her consent and whether the third party is capable of giving consent or has expressly refused consent. These principles would apply to any reference held on an employee's personnel file that had been supplied by a previous employer.

The employer must respond to a subject access request without "undue delay" and at the latest within one month of receipt of the subject access request. If the request is complex, the employer can extend the time limit for responding to three months.

What principles are employers obliged to follow to ensure that personal data is handled correctly?

Employers are obliged to adhere to the data protection principles set out in the General Data Protection Regulation (GDPR), which is in force from 25 May 2018. These state that employers must:

- process personal data lawfully, fairly and in a transparent manner (which means that personal information must not be obtained or used unless one of a limited range of legal grounds for processing applies);
- obtain and process data only for specified, explicit and legitimate purposes;
- ensure that data is adequate, relevant and limited to what is necessary in relation to its stated purpose (i.e. collect and store only the minimum information necessary);
- ensure that data is accurate and kept up to date and take every reasonable step to ensure that data that is inaccurate is erased or rectified without delay;
- not keep data for longer than is necessary for the purpose for which it is processed; and

- process data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

Employers must be able to demonstrate their compliance with these data protection principles under the GDPR.

Does an employee who believes that she may have an equal pay claim have the right to be given information about her male counterparts' salaries?

An employee does not have the right to be given information about her male counterparts' salaries for the purpose of deciding whether or not she has a valid equal pay claim. However, if she does bring a claim, she may seek an order from the tribunal for disclosure of documents relating to comparators. The tribunal will consider the relevance of any documents before deciding whether or not it will order disclosure.

If an employee asks the employer for comparators' salary information before bringing proceedings, the employer may wish to disclose this, for example where it could show that the employee does not have grounds for a claim. However, there is a difficulty for employers in that salary information is regarded as confidential and is itself covered by the GDPR. This is a difficulty that has not yet been fully resolved by the courts and tribunals. In some cases, an employer may be in a position to disclose comparators' salary information while still preserving their anonymity. If a tribunal has ordered disclosure of information the employer will be disclosing it because it is necessary to comply with a legal obligation, and therefore will not be in breach of the GDPR.

Section 77 of the Equality Act 2010 makes pay secrecy clauses in an employee's contract unenforceable if the employee is involved in a discussion to establish if differences in pay exist that are related to a protected characteristic such as sex. While this provision means that employers cannot prevent employees from providing information about their salary to a colleague, employees are under no obligation to provide such information.

How does the act affect keeping of employment records?

The Data Protection Act and the General Data Protection Regulation will generally apply to all information kept we keep about employees.

The legislation does not prevent the collection, maintenance and use of employment records. However, it helps to strike a balance between the need to keep records and the employee’s right to respect for their private life.

The legislation requires openness. Employees should be aware what information is being kept about them, and what it will be used for, and if it will be disclosed. This information is covered in the HR Privacy Notice.

All those with access to employment records must be aware that data protection rules apply and that personal information must be handled with respect.

We should not keep information that is excessive, irrelevant or out of date. Any information that there is no genuine business need for, or a legal obligation to keep, should be destroyed in accordance with the HR retention schedule.

Data protection does not stand in the way where there is a legal obligation to disclose information, for example the Inland Revenue regarding payments to employees. Nevertheless, you should be careful not to divulge more information than is required.

Employees should have the opportunity to verify their own records periodically. This allows mistakes to be corrected and information to be kept up to date.

All employment records should be kept secure. Paper records should be kept under lock and key and computerised records should be password protected. Only employees with the proper authorisation and necessary training have access to employment records.

Managers retaining their own personnel files

The ICO advise that some records, in particular sickness records containing details of an employee's illnesses or medical conditions should be retained separately than other, less sensitive information. Where managers genuinely require access to health records in order to carry out their job, this is acceptable but records must be kept securely, under lock and key or password protected.

Should employers ask job applicants for consent to process their data under the GDPR?

Provided that the processing is limited to what is necessary for the recruitment process, there is no need to ask job applicants for their consent to process their personal data under the General Data Protection Regulation (GDPR).

We must be able to demonstrate that we have a legal basis under the GDPR to process personal data. In the case of personal data provided by job applicants as part of a recruitment process, the legal basis is that 'processing is necessary for the purposes of the legitimate interests of the employer'. We as the potential employer need to process personal data provided by candidates when conducting the recruitment exercise; for example, to assess and record information about their qualifications as part of the selection process. We have a legitimate interest in managing the recruitment exercise effectively to decide to whom to offer a job. We are also under a legal obligation to process certain information as part of a recruitment exercise, for example, checking that a successful candidate has the right to work in the UK.

There is therefore no need to obtain candidates consent for the processing as an additional or alternative legal basis.

We provide candidates with a privacy notice, setting out, among other things, the purpose and the legal basis for processing their data, and their right to object to the processing in certain circumstances.

What information must employers supply to employees about the processing of their personal data under the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation requires us to provide employees (and other data subjects, such as job applicants) with a privacy notice, also known as an information notice or fair processing notice, setting out specified information about the processing of their personal data. This must be provided when we collect personal data from the employee or use the personal data for a new purpose. The information that the employer must provide under the GDPR is significantly more detailed than that currently required under the Data Protection Act 1998.

Under the GDPR, the employer's privacy notice must include:

- the identity and contact details of the employer as the data controller;
- the data protection officer's (DPO) contact details (if the organisation has a DPO);
- the purposes for which the data will be processed and the legal bases for processing;

- where the legal bases for processing is the legitimate interests of the employer or a third party, the legitimate reasons relied on;
- the recipients, or categories of recipients, of the data, if any;
- details of any transfer of the data outside the European Economic Area and the relevant safeguards in place;
- the period for which the data will be stored, or if it is not possible to specify the retention period, the criteria used to determine the period;
- the data subject's rights to request access to, rectification or erasure of data; to request restriction of processing; or to object to processing;
- the right to data portability;
- where the legal basis for processing is consent, the right to withdraw consent at any time;
- the right to lodge a complaint with the supervisory authority;
- whether or not the provision of personal data is a statutory or contractual requirement, and the possible consequences of failure to provide the data; and
- the existence of any automated decision making and profiling, and the consequences for the data subject.

Where the data was not obtained directly from the employee, the employer must also state the source from which it was obtained and the categories of personal data to be processed.

What is the right to be forgotten under the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation provides individuals with the right to request the erasure of personal data concerning them, also known as "the right to be forgotten". Employers will be obliged to erase personal data relating to an individual if:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the individual withdraws his or her consent and there is no other legal ground for the processing;
- the individual objects to the processing of data where the processing is on the basis of the employer's legitimate interests and there are no overriding legitimate grounds for it to continue;
- the personal data has been unlawfully processed; or
- erasure is required for compliance with a law to which the employer is subject.

If one of the above grounds applies, the employer must erase the personal data without undue delay, on the request of the individual.

If the employer has made the personal data public, it also has a duty to take reasonable steps to inform other data controllers that are processing the data that the individual has requested the erasure of the data and any links to or copies of it.

In the employment context, processing of employee data is necessary to maintain the employment contract. After an employee leaves, their records are retained in accordance with the HR retention schedule.

For how long should an employer keep an employee or ex-employee's personnel files?

The General Data Protection Regulation sets no specific periods for retention of employees' personal data, but one of the key principles of the GDPR is that personal data should not be kept longer than is necessary for the purpose or purposes for which it is being processed.

Employee records are kept in accordance with the HR retention schedule, although currently, due to the on-going Independent Inquiry into Child Sex Abuse, no employee files are being destroyed until further notice.