General Data Protection Regulation (GDPR) Policy

Competition Service

Date Last Reviewed	March 2018

Table of Contents

1 Introduction

The General Data Protection Regulation sets rules for the processing of personal information. GDPR gives certain rights to individuals – the 'data subject' – but also places responsibilities on those who handle personal data on others.

Any information about a living individual is '**personal data**'. The information can include expressions of opinion and future intentions in relation to someone. It can be about an unnamed person if he or she can be identified from other information in the Competition Service's (the Service) possession.

With the introduction of the General Data Protection Regulation (GDPR), an emphasis has been placed on consent and any subsequent removal of consent by the data subject which needs to be closely monitored by the data controller.

2 SCOPE

This policy applies to all employees. It does not apply to contractors, temporary workers or those not directly employed by the Service.

3 LEGISLATION FRAMEWORK

The following Acts, such as they apply, will, so far as reasonable, be taken into consideration when implementing this Policy:

- Data Protection Act 1998
- GDPR

4 PRINCIPLES OF INFORMATION HANDLING

There are eight enforceable principles of good practice. The data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in line with the individual's (the "data subject's") rights;
- Secure;
- Not transferred to countries without adequate protection.

The Service must follow these principles.

5 RESPONSIBILTIES IN THE SERVICE

In the Competition Service the appointed **Data Protection Officer** is the Director, Operations. The Service itself is the **'Data Controller'** registered with the Information Service. The Data Protection Officer is responsible for implementation of GDPR insofar as it affects personal data on Service members and staff (including period appointees and contractors). In particular the Data Protection Officer is responsible for:

- Ensuring day-to-day compliance with GDPR;
- Advising on data protection policy as it impacts on the Service's staff records;
- Advising the Registrar about changes required to the Service's registration with the Information Service;
- Facilitating responses to data subject access requests from Service's members, staff, and the general public; and
- Liaising with the Service's legal advisers and the Office of the Information Service, where necessary.

It is important to remember that all staff who record or hold information about others have a responsibility to do this in accordance with the provisions of GDPR and any guidance issued by the Data Protection Officer. More details are given at Para 7.

6 YOURS RIGHTS AS AN INDIVIDUAL

6.1 Your rights

GDPR gives you a number of rights, including:-

6.1.1 The right of subject access

GDPR allows an individual – the 'subject' - to find out what information is held about themselves on computer and some paper records. This is known as the right of subject access.

6.1.2 The right of rectification, blocking, erasure and destruction

GDPR allows individuals to apply to the Court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

6.1.3 The right to prevent processing

A data subject can ask a data controller to stop or request that they do not begin processing data relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else (though this right is not available in all cases and data controllers do not always have to comply with the request).

6.1.4 The right to compensation

A data subject can claim compensation from a data controller for damage, or damage and distress, caused by any breach of GDPR. Compensation for distress alone can only be claimed in limited circumstances.

6.1.5 Rights in relation to automated decision-taking

An individual can ask a data controller to ensure that no decision which significantly affects them is based solely on processing his or her personal data by automatic means. There are, however, some exemptions to this.

6.1.6 Exercising your rights

You may exercise your rights in the following ways:

(a) Information held by Human Resources Department.

Details of the records held in by HR are set out in Appendix 1. If you wish to exercise your right to see information to which you are entitled you should write to HR giving your:

- Name;
- Telephone Number;
- Date of Birth;

- National Insurance No.;

and setting out (so far as possible) details of the data to which you want to have access.

In some cases it may be easier for you to look at papers or other records before deciding which ones you want copied. Where you prefer to follow this option the Data Protection Officer will normally:

- Make an appointment for you to come and view the file(s);
- If necessary, secure a quiet room where you can look at them;
- Arrange that either he or she, or one of their staff, is present throughout the time that you are looking through the file. (For obvious reasons it will not be permissible for any documents to be removed from files);
- Make a copy of any documents you request and send them on to you;
- Deal with any questions you may have about the contents of the file(s) at the time. Where this is not possible, another meeting will be arranged or you will receive a letter about the point at issue.

(b) Information held by your Line Manager

If you wish to exercise your subject access rights in relation to records that you believe to be held by your line manager, instead of following the procedure set out above you should:

- Ask your line manager for the information you require, or to let you see the records you wish to see;
- If your line manager wants the matter handled on a more formal basis, make a request to him/her in writing;
- If your line manager considers that your request goes wider than the data he/she holds, he/she will refer you to the Data Protection Officer.

6.1.7 Retention periods for Personnel records

Personnel records are kept for varying periods according to need. The Data Protection Officer will give you further information on this point if you wish.

6.1.8 Constraints on requests for access

There are constraints on the number and frequency of requests that can be made. GDPR provides for you to have access to your personal data provided the requests are made “at reasonable intervals” and “are not similar” (i.e. if you apply for access to your sick leave record every other week then these requests are similar but, if you apply for access to your sick leave

record and then for details of your staff reports, then these are not similar). Three things will be considered when deciding whether repeated requests for information are reasonable:

- the nature of the personal information;
- the purpose for which the information is held;
- how often the information is altered.

Where we have already complied with an identical or similar request by you, we are not obliged to comply with the further request unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request. If you repeatedly apply for the same data the Service reserves its right under GDPR to charge you for processing each request.

6.1.9 Limitations on access rights

Apart from the question of numbers and frequency of requests, there are some important exceptions to your rights of access. These are set out in Appendix 2.

7 YOUR RESPONSIBILITIES AS A MEMBER OF THE SERVICE'S STAFF

7.1 All Staff

1. As noted earlier, all staff have a duty to observe the provisions of the legislation as well as rights which they can exercise on their own behalf. The principles underlying information handling were spelt out above at paragraph 4.

   If someone asks for copies of their personal data, the first thing that has to be done is to identify the files that refer to them. When those files have been identified, the Data Protection Officer has to go through them to identify the information to which that person is entitled to have access, and any other information that we are willing to disclose voluntarily. When a request is received, ideally IT should be able to find the relevant files that are held electronically by carrying out a search using a single word, e.g. the person's surname. This would not be possible if there is personal data on a Windows Explorer drive or a mobile device or on a file that does not mention the name of the person but, for example, refers to him by his initials. In the light of this, **it is particularly important that you are aware of the steps you should take in relation to information which you hold or create on your computer. The following points are especially relevant:**

2. Avoid having files on your Windows Explorer drive or mobile device that contain personal data;

3. Regularly delete those of your files that contain personal data from Windows Explorer drives. The same applies to sent and received e-mails in Outlook. The deleting of files and e-mails as soon as they are no longer needed reduces the work involved in handling a request under GDPR, and it is consistent with the law. Deleting should take place **unless -**

   - they need to be kept for operational purposes, or

   - they are being kept for "research (including historical) purposes".

4. If you are minded to retain a file on the office computer system for research (including historical) purposes, make sure you comply with paragraphs 3, 4 and 5 of Appendix 2.

5. Make sure that you delete files from the recycle bin on your desktop and from Deleted Items in Outlook.

6. Ensure that any file that contains personal data contains the surname of that person (so that a word search can easily find it); if it is not in the text of the document insert it in "Properties" as a comment.

7.2 Line Managers/Reporting Officers

Matters of particular relevance to Line Managers and Reporting Officers are set out in Appendix 3.

APPENDIX 1 RECORDS HELD BY THE HUMAN RESOURCES DEPARTMENT

HR hold the following records on all staff:

(a) ***Personal file*** (contains in general terms information on pay, pensions, recruitment, transfers, employment details and career);

(b) ***Reports file*** (contains performance appraisal reports and promotion board assessments covering the last 6 years);

(c) ***Sick absence file*** (contains sick leave certificates and related documentation);

(d) ***Computer printouts*** on each member of staff containing such details as name, date of birth, address, NI number, and next of kin.

In addition, a limited number of HR staff may have one or more of the following files:

(e) ***Medical file*** (containing papers relating to long-term ill health affecting employment);

(f) ***Conduct and Discipline file*** (containing papers relating to the process and outcome of formal disciplinary proceedings);

THE FOLLOWING IS A GUIDELINE FOR RETENTION OF INFORMATION

Document	**Time Guideline**
Application Form	Duration of employment
Payroll and Tax information	6 years
References received	1 year
Sickness records	3 years
Annual leave records	2 years
Annual appraisal/assessment records	5 years
Unpaid leave/special leave records	3 years
References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, eg name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

APPENDIX 2 EXEMPTIONS TO RIGHTS OF ACCESS

The main permitted exclusions from the provisions of GDPR of relevance in this area are as follows:

- Personal data processed for the purposes of **management forecasts** or **management planning** to assist the Service in the conduct of its activities are exempt from the subject information provisions to the extent to which the application of those provisions would be likely to prejudice the conduct of that activity. Once the time covered by a forecast has passed or a plan has been put into effect it may be difficult to see how the business or other activity can be prejudiced and this exemption may not apply.

- Personal data which consists of records of the intentions of the Service in relation to any **negotiations** with the data subject are exempt from the subject access provisions to the extent to which the application of those provisions would be likely to prejudice those negotiations.

- Personal data which consists of a **confidential reference** given or to be given by the Service for the purposes of education, training or employment, appointment to office or provision of any service are exempt from subject access rights (although, once given, the subject may have access rights with the recipient).

- Personal data processed for the purposes of assessing a person's suitability for **judicial office** or conferring any **honour** are exempt from the subject information provisions.

- Personal data is exempt from most provisions if the exemption is required for the purpose of safeguarding **national security**; and

- Personal data consisting of information in respect of which a claim to **legal professional privilege** could be maintained in legal proceedings (eg confidential communications between the Service and its legal advisers) is exempt from the subject access provisions.

- Personal data relating to **crime** and **taxation** may be exempt; and

- **Information kept <u>only</u> for research** purposes (see para 2 below) can be kept indefinitely and does not have to be disclosed to the data subject though the

exemption does not apply if the information is used or being kept to support measures or decisions with respect to particular individuals.

The definition of **'research purposes'** includes 'historic purposes'.

If you want to be able to claim that a file is being kept on the office computer system for research purposes, you need to be in a position to demonstrate to the Information Service or the courts that it really is being kept for that purpose and that it is not, for example, on the system simply because you never got round to deleting it when it was no longer needed. You should, therefore, ensure that there is an audit trail that can be used to demonstrate that it is being kept for that purpose.

As this exemption can give rise to policy and legal issues, you should consult the Data Protection Officer if you wish to use this particular provision.

APPENDIX 3 WHAT YOU NEED TO DO AS A LINE MANAGER/REPORTING OFFICER TO ENSURE YOU COMPLY WITH THE PRINCIPLES OF GDPR

First, you should ensure that your local sources of data on staff (folders or casual records, both manual and electronic) meet all of the principles. If they do not, you should take action to ensure that they do.

In particular, you need to have good housekeeping arrangements in place to ensure that your Department or Group processes personal data legitimately, fairly and securely. For example, you may hold notes on a member of your staff's performance to help you compile his or her annual report. You should ensure such information is properly secure, that it is relevant to the purpose, not excessive, and is not kept longer than is necessary. This is because you could at some point be asked to justify your arrangements for the retention and destruction of data.

You should especially ensure that:

- you do not hold "sensitive" personal data on individuals locally. "Sensitive" personal data is defined GDPR as racial or ethnic origin; political opinions; religious or similar beliefs; TU membership; physical or mental health; sexual life; and data relating to criminal offences. Only the Registrar or the Data Protection Officer can authorise any departure from this rule;

- the records you hold locally are accurate and fair and that any papers that are not otherwise exempt from disclosure are suitable for disclosure to the relevant individual on request;

- manual personnel records are stored and handled in accordance with security guidelines; and

- records are held no longer than necessary, and certainly no longer than is consistent with the Service's retention policy, and that they are destroyed promptly and with due care once they have fulfilled their purpose.

RETAINING DOCUMENTS

The retention of personal data is largely a matter of commonsense. In essence it should not be retained unless there is a clear business need, or the Service's interests would somehow be damaged if it were not retained. In practice very little should be held beyond documents relating to performance assessment, disciplinary issues, career development and training needs or information about absences. There should be no need to retain "unofficial" notes or records about colleagues, and nothing should be retained that you are not prepared to have revealed to the individual concerned.

There are circumstances, however, when it will be prudent to retain information for longer periods—for example, information needed to support inefficiency proceedings or a disciplinary issue where a historical record would be useful should behavioural weaknesses re-surface (for example, harassment and bullying issues). But even here time limits can apply, and the schedule attached sets out recommended retention periods for the types of personal information you may hold as line managers.

In practice, local personal data will probably only be accessed by the individual themselves, their line manager or their countersigning officer. If anyone else is likely to have access, (and there

would need to be good reason for this) the data subject should be told who it is, and why they will have access to their personal data. Of course, there will be occasions when another person is provided with information because it follows from a request made by the individual (for example, if a member of staff asks that information should be given to a line manager in another Department to support a request made for a secondment). In those circumstances the sending of that information will be done with the full agreement of the individual, and will be consistent with the provisions of GDPR.

WHEN STAFF MOVE

When a member of staff transfers to another line manager, the exporting and importing line manager should discuss whether it is appropriate to transfer any personal data to the new line manager. These should generally only relate to live actions which the new manager is required to take forward. Any personal data not transferred should be destroyed by shredding by the person holding the data.

EX-STAFF

Line managers should not retain any personal data on staff who have retired, resigned or been dismissed from employment with the Service for longer than three months after they have left. Should they hold any top copies of documents, these should be returned to the HR Department so that they can add them to the official record.

PERSONAL DATA ARISING FROM REFERENCES OR APPEALS

In the course of their work Inquiry Teams and Appeal Tribunal staff will acquire a certain amount of data on the home addresses, private telephone numbers, mobile and fax numbers, e-mail addresses of representatives of the principal parties, and from third parties as well.

Where this information is filed as part of general files (i.e. it is not filed by reference to individuals, or in such a way that information relating to individuals is readily accessible), it would not form part of a relevant filing system and would not therefore be covered by GDPR. Such general files would continue to be reviewed and destroyed using the Service's current criteria.

The Service's disaster recovery plan states that principal parties' main contacts with the Service should be kept in case of emergency. Once the reference has been completed, and it is clear these details are no longer required, they should be disposed of.

HOME ADDRESSES AND TELEPHONE NUMBERS

Many line managers will have lists of home addresses and telephone numbers of contractors, short-term appointees and certain members of staff. Where this information has been given willingly by the individuals concerned, where its retention may be of future benefit both to them and the Service, and where no other data is kept, no interests are likely to be damaged, and there is unlikely to be any challenge to the details being retained. Line managers will want to use their own good sense in weeding this material.

CONTRACTORS

Papers relating to directors, partners, or members of staff of contractors or individual contractors that form part of a relevant filing system should be retained for no longer than six years.

LITIGATION

Documents must not be destroyed if they could be relevant in any contemplated or actual litigation (including criminal proceedings). This overrides any of the previous paragraphs. In certain circumstances destruction could result in proceedings for contempt of court.

WEEDING OF FILES

As a matter of course you should weed your local records when they are next referred to for action.

Files must not be weeded after a request has been made but before the information is supplied. Such action could result in there being a contravention of GDPR. This is because GDPR requires the data subject to be provided with information concerning his personal data as at the time he or she requests it (although account can be taken of routine amendments and deletions that would have been made regardless of the request).

ACTION TO BE TAKEN ON RECEIPT OF A REQUEST FOR DATA

The following steps outline the process you should follow when you receive a request for data:

(a) If the request is made orally and relates to information held by the HR Department or outside your command, tell the person to send his or her request to the Data Protection Officer. Otherwise, decide whether the matter can be handled on an informal basis outside the terms of GPR. If you decide that handling the request on an informal basis would not be appropriate, ask for the request to be made in writing or by e-mail.

(b) If the request is in writing or by e-mail and relates to information held by the HR Department or outside your command, you should pass it to the Data Protection Officer immediately.

(c) Where the request relates to information you personally, or your Department or Group, hold on the individual you should send a copy of the data to that person along with any necessary explanatory notes. This must be supplied promptly and in any event within 40 calendar days of receiving the request—or clarification of this request, should this be necessary. This sub-paragraph does not apply where an exemption is applicable or third party rights are affected (see paragraph 19 below).

(d) You should draw attention to any inaccuracies in the data and explain why they have occurred and the steps you are taking to correct them. You should not alter the inaccuracies after you have received the request. The data must be passed on in this state. Only when the individual has seen the data and agreement has been reached on the amendments needed should it be changed.

(e) Where there is a need for some discussion about, or some further explanation of, the data, you should arrange a meeting with the individual concerned to work through the issues of concern.

(f) You must satisfy yourself as to the identity of the person making the request in order to ensure that the information does not go to a third party. For example, if a person makes a request by e-mail you should not provide the information by e-mail without first satisfying yourself that the e-mail was sent by the person who purported to send it.

Similar procedures apply where the initial request is made directly to the Data Protection Officer.

THIRD PARTIES

There may be cases where complying with a subject access request would involve disclosing information relating to an individual other than the data subject. This applies not only in cases where the third party is named but also where the third party can be identified from the information supplied and any other fact known to the data subject. For example, for most staff, their line manager will hold only contact details and information relating to the member of staff's performance appraisal, training and development. However, there may be circumstances when others have offered comment: e.g. an informal complaint or grievance (e.g. "in relation to the incident A N Other has provided the following information …"). The fact that A N Other gave this information is A N Other's personal data. The same could apply if A N Other was not named but the data subject would know that there was only one person who could have provided the information.

The Service would not be obliged to disclose this kind of information unless either:

- the third party individual had given his consent; or
- it would be reasonable in all the circumstances to comply with the request without his consent.

In some cases you may be in a position to obtain the consent of the third party. In others you may be able to negotiate an amicable solution acceptable to all concerned. However, the decision on whether to refuse access on these grounds or to disclose another individual's personal data without his consent must be referred to the Data Protection Officer.

EXEMPTIONS

The fact that an exemption applies to information does not necessarily mean that it cannot lawfully be disclosed to the data subject. In the case of some of the exemptions it would clearly be inappropriate. However, in the case of, say, confidential references or legal professional privilege, there could be circumstances where the information could properly be disclosed.

WHAT HAPPENS IF YOUR STAFF DECIDE TO INVOKE THEIR ADDITIONAL RIGHTS?

As well as providing new rights of access to data, GDPR provides other rights. These include the right to prevent processing likely to cause damage or distress; and the right to take action to rectify, block or destroy inaccurate data.

If you receive a request in respect of any of those other rights, would you please refer them to the Data Protection Officer for advice.

RETENTION PERIODS FOR PERSONAL DATA HELD BY **LINE MANAGERS**

Personal data held by line manager to which individuals may request access under GDPR	*Copies should be retained for no longer than*
Current home address details	**Employee leaves your section**
Recruitment papers: • **Routine appointments** • **Fixed term appointments/short-term contract**	**12 months** **Duration of the contract**
Annual/Assessment Reports • **Material compiled for use in report** • **Annual reports**	**Once the report for that year has been compiled and signed off** **2 years or when employee leaves your Department or Group**
PAP reviews	**2 years or when employee leaves your Department or Group**
Data relating to inefficiency or disciplinary action	**Once the cycle of action has been completed**
Annual Leave records	**2 years or when employee leaves your Department or Group**
Job applications – internal	**12 months**