NORTH YORKSHIRE
FIRE & RESCUE SERVICE

Data Subject Rights Request Procedure

North Yorkshire Fire & Rescue Service
Headquarters
Thurston Road
Northallerton
North Yorkshire
DL6 2ND

Tel: 01609 780 150

www.northyorksfire.gov.uk

VERSION CONTROL TABLE

Date of Issue	Version Number	Status
14/04/2018	0.1	Draft based on GDPR
2/05/2018	1.0	Approved by IGG
22/05/2018	1.1	Draft (Based on resource changes)

TABLE OF REVISIONS

Date	Section	Revision(s)	Author
14/04/2018	0.1	Draft based on GDPR	CAO Manger and IG Officer
22/05/2018	1.1	Minor amendment to CAOM duties and inclusion DPO contact details	CAOSI Lead

CONTENTS

INTRODUCTION

The General Data Protection Regulation (GDPR) supplemented by the forthcoming Data Protection Act[1] regulate the use of living individual's (data subjects) personal data and provide a data subject with certain rights. Not all rights are absolute and can be subject to exemptions.

PURPOSE

The purpose of this procedure is to set out how a data subject can make a rights request in regards to their personal data, provided for by GDPR Articles 15 - 21, and how North Yorkshire Fire & Rescue (the Service) will deal with requests involving personal data. In particular:

- To ensure good practice in dealing with personal data rights requests.
- To ensure compliance with the GDPR and other applicable legislation and regulation related to personal data.

The Service will ensure that all responses to 'data subject rights requests' comply with relevant local and international regulations on data protection and information security, and those responses are in the interests of both the subject and the Service.

Specifically, where personal data is being processed by the Service and the identity of the data subject has been confirmed, the Service shall respond to the request and provide the data subject with a response.

SCOPE

This procedure applies to staff, contractors, consultants, temporaries, and other workers at the Service including all personnel affiliated with third parties.

It covers the following rights requests involving personal data including:

- access requests (GDPR Article 15);
- rectification requests (GDPR Article 16);
- erasure requests (GDPR Article 17);
- right to restrict processing (GDPR Articles 18);
- transfer (portability) requests (GDPR Article 20).
- Rights to object to processing (GDPR Articles 21)

This procedure should be read in conjunction with the Data Protection Policy.

RESPONSIBILITIES

All employees have a responsibility to adhere to this procedure regardless of their status.

The CAO Manager has direct responsibility for maintaining this procedure and providing advice on implementation with assistance of the DPO as required.

The CAO Service Information team (CAOSIT) is the dedicated team responsible for processing data subject rights requests, so should you have;

- Queries surrounding the procedure;

[1] The Data Protection Bill is currently going through the House of Lords, this procedure will be updated after it has come into force

- As a member of staff, receive a request;
- Or if you are unsure whether you have received a request;

Please contact the **CAO Service Information Team**, whose details are provided under 'Make a Rights Request'

PERSONAL DATA DEFINTION

It is useful to understand what constitutes personal data for the purposes of this procedure.

Personal data means any information relating to an **identified** or **identifiable** living individual who can be **identified, directly or indirectly**. Personal data includes facts, opinions or intentions relating to the individual. This individual is known as the 'data subject'.

The Regulation applies to personal data which;

- Is processed wholly or partly by automated means e.g. computer, CCTV, voicemail
- forms or intended to form part of a structured filing system e.g. categorised file that enables your details to be readily accessible according to specific criteria
- is recorded by a public authority e.g. manual unstructured data but with certain caveats

The Information Commissioner's Office 'Guide to the General Data Protection Regulation (GDPR)' provides an outline of the Key Definitions

TYPES OF PERSONAL DATA PROCESSED

To provide an effective emergency service and safeguard communities the Service process a range of personal data. Examples of when personal data is processed include;

- during 999 calls, including mobilisation of fire engines
- attending incidents and investigating the causes of fires
- during Safe and Well or Home Fire Safety visits
- running education / training programmes for young people
- recruitment and employment records
- responding to telephone and written enquiries.

The personal data obtained could include (but not limited to);

- name, address, email address, gender, age, ethnicity
- details about risks in an individual's home (such as smoking, use of oxygen or disabilities)
- job performance
- pay and bank details
- posts on social networking sites, including your online name

MAKING A RIGHTS REQUEST

A data subject rights request can be made via any of the following methods:

- Verbally
- Fax
- Social media
- Email
- Post
- Corporate website

The "Data Subject Rights Request Form" can be provided to a requestor to submit a request or alternatively they can telephone **CAOSIT** on 01609 780150.

A copy of the form can be found in Appendix A.

The Service advises requestors to include as much information as they can to assist in locating their data. If the request is surrounding access to personal data, the Service may request that the requestor specifies the data that the request relates to, if a large volume of data is held.

Postal address:
CAO Service Information
North Yorkshire Fire and Rescue Service
Service Headquarters
Thurston Road
Northallerton, North Yorkshire
DL6 2ND
Email: cao.serviceinformation@northyorksfire.gov.uk
Telephone: 01609 780150 **Fax:** 01609 788520
Via the Service Website: here

In the event that a data subject wishes to make their request via Twitter or Facebook, the addresses are below;

Twitter: twitter.com/NorthYorksFire

Facebook: www.facebook.com/northyorksfire

Requests made via social media must be treated like any other request when they are received however, the Service will not provide a response via any social media channels.

If a data subject requires any assistance in making a request or has a disability and requires reasonable adjustments to make a request, please phone the **CAOSIT** on 01609 780150 who can discuss it with them.

Requests from members of the public
Members of the public may ask any member of staff how they can exercise their data subject rights, staff should either direct the requestor to the **CAOSIT** (contact details above) or to the Service website page on your information (data protection). An application form to access their information is also available here.

Requests from staff
If staff members request personal data that the Service may hold (i.e. HR / personal file) then these must be directed to **CAOSIT** and treated the same as a request from a member of the public.

IDENTIFICATION

The data subject must prove their identity prior to any disclosure of any information to them, in the form of a full valid driving licence, a birth certificate, a full valid current passport **and** a gas, electricity, water or telephone bill in their name for the last quarter.

The ID can be photocopied and posted to the Service or it can be scanned and emailed.

Where there are any reasonable doubts concerning the identity of the data subject, additional information will be requested by the **CAOSIT** to confirm the identity of the data subject.

Once the Service is satisfied a note will be made that this requirement has been met and the copies of identification documents will be shredded. Any originals will be sent back via recorded delivery.

NB: Member of staff ID checks – the **CAOSIT** needs to check the identity of anyone making a request to ensure information is only given to the person entitled to it however, if the member of staff confirms the request to **CAOSIT** no further checks are required.

If the Service can demonstrate that it is not in a position to identify the data subject, even if additional information is provided to assist with identification, a refusal notice to act upon the request will be issued.

REQUESTS FROM PARTIES OTHER THAN THE DATA SUBJECT

There are occasions whereby a data subject may agree to a third party making a request, such as a solicitor, somebody looking after their welfare or a potential employer. To protect a data subject's data, the Service will make all the necessary checks to satisfy it that the individual making the request on behalf of the data subject is entitled to do so. This may include requesting a written authority to make the request (e.g. evidence of consent from the individual) or a more general power of attorney. No information will be released until the Service is satisfied.

The Service may feel it appropriate to contact an individual directly to discuss the request, for example, if asked to release their medical record file. On an occasion such as this, the data subject will be given an overview of the type of information that will be released and the option to;

- see their personal data first and upon consent it will be released to the third party
- grant permission for it to be sent directly to the third party
- withdraw consent and no information will be sent to the third party

REQUESTS FROM PARENT / GUARDIAN / CARER

Requests can be made, but it has to be recognised that the personal data is that of the child's, and that they have exactly the same rights as anyone. The Service will take into consideration whether it's in the best interest of the child to release the data or take action on the request. In the majority of cases, where the Service considers the child to understand their rights, the child will be contacted directly.

Prior to any action the Service will request proof of parental responsibility, for example, birth certificate or passport.

The Service will take the approach that a child aged 13 years has the capacity to make a rights request.

FEES

In the majority of cases there will be no fee for acting upon a request, however where the Service can demonstrate that the request is manifestly unfounded or excessive in nature it can either;

- Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

- Refuse to act on the request.

A data subject will be informed of such decision, the reason why, how a complaint can be raised with the Information Commissioner's Office (ICO) and how to seek a judicial remedy if desired.

If the request relates to access to personal data, where the Service has provided one copy of the personal data free of charge, for further copies of the data, the Service shall charge a reasonable fee to the data subject based on administrative costs.

The administration cost would include actions such as photocopying charges.

RESPONSE TIMES

The Service shall provide a response to the data subject without undue delay and in any event within one month of receipt of the request.

This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. **CAOSIT** shall inform the data subject of any extension within one month of receipt of the request, together with the reasons for the delay.

If it is not possible to action the request of the data subject, **CAOSIT** shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint to the ICO and seeking a judicial remedy, if desired.

RESPONSE FORMAT

The data in any response shall be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The response shall be provided in the medium requested by the data subject or representative where possible. Where no medium has been specified, the response shall be:

- In writing, for requests received in writing;
- In electronic form, by using the secure email system (Egress), for requests received via email;
- Provided orally, for requests received orally.

RESPONSE TO ACCESS REQUESTS

This right enables a data subject to verify that the Service is lawfully processing their personal data and to check its accuracy.

Where data is being processed by the Service and the data subject makes a request to access the data, the Service shall provide the data subject with access to the personal data and, provide:

- The purposes of the processing;
- The categories of personal data concerned;

- The recipients or categories of recipient to whom the personal data have been or will be disclosed (where transferred outside the EU, include the appropriate safeguards relating to the transfer);
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from NYFRS the rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with the ICO;
- where the personal data is not collected from the data subject, any available information as to their source;
- Any existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Where personal data is transferred to a third country or to an international organisation, the appropriate safeguards relating to the transfer.

The Service has a duty to ensure other individual's information is treated fairly or protected accordingly. Therefore, before the Service releases anything to the data subject or representative it has to ensure that it's not inappropriately releasing information about another individual who can be identified from that information.

On occasions where somebody else can be identified from that information, the Service will not release data relating to the data subject unless the other individual has consented to the release of the information or it is reasonable in all circumstances to release the information without consent.

The Service will take the below approach;

- Seek documented consent from other individuals
- Where appropriate redact (blank out) information so other individuals cannot be identified, such as names / addresses/ identification
- Where appropriate provide a summary of the personal data
- Review whether it would be reasonable to release the information without consent. The Service would ask itself a range of questions, such as; is the information already known by the data subject? Is the individual acting in their professional capacity and had dealings with the data subject? Is there a duty of confidentiality owed to the other individual?

The data subject's interests and that of the other individual will be reviewed and considered. The Service would give regard to; The Regulation, forthcoming Data Protection Act, Article 8 The Human Rights Act (1998) and the CASE OF GASKIN v. THE UNITED KINGDOM judgement.

All decisions will be made on a case by case basis, taking into consideration other legislation that may force the release of information to the data subject.

As an additional safeguard for the data subject, the forthcoming Data Protection Act is likely to make it an offence to intentionally conceal all or part of a data subject's data.

RESPONSE TO RECTIFICATION REQUESTS

Where the request is for the rectification of inaccurate personal data, the Service shall carry this out without undue delay where the request does not conflict with any legal, regulatory or other such constraints. This may include updating personal data to include a supplementary statement.

The Service will restrict further processing of your personal data whilst it verifies the accuracy.

Where the rectification request is upheld, the Service shall inform any third parties who have been sent personal data that the data subject has made a rectification request and instruct all parties what rectification is required. The exception to notifying third parties is if this proves impossible or involves disproportionate effort.

The Service shall inform the data subject of such third parties if they request this information.

RESPONSE TO ERASURE REQUESTS

When requested to do so by the data subject, the Service will erase personal data without undue delay where the request does not conflict with any legal, regulatory or other such constraints.

The table below details when the obligation arises and when it doesn't.

Obligation to erase personal data where;	**Obligation doesn't apply if the processing is necessary for;**
It's no longer necessary for the purposes for which it were collected or processed	Exercising the right of freedom of expression and information
The processing is based on data subject consent and it's been withdrawn, and there is no other legal ground to process	Compliance with a legal obligation
The data subject has successfully objected to the processing of their personal data **(see response to objection requests)** and now request it to be erased	The performance of a task carried out in the public interest or in the exercise of official authority vested in the Service (statutory functions)
It's been unlawfully processed	Reasons of public interest in the area of public health and processed in accordance with the Regulation
It's to be erased for compliance with a legal obligation	Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and erasure would likely render impossible or seriously impair the achievements of the objectives of that processing
It's collected in relation to the offering of an information society service to a child	Establishment, exercise and defence of legal claims.

Where the erasure request has been upheld, the Service shall instruct third parties that have been sent personal data that the data subject has made a request for erasure. The exception to notifying third parties is if this proves impossible or involves disproportionate effort.

If the Service has made the personal data public on an online environment, it will take all reasonable steps to inform other organisations who process the personal data that the data subject has requested **erasure** of any links to, or copies or replications of the personal data.

The Service shall inform the data subject of such third parties if they request this information.

RESPONSE TO RESTRICTION REQUESTS

The data subject shall have the right to restrict 'block' processing of their personal data.

Methods adopted by the Service to restrict the processing could include, temporarily moving the selected data to another system, making it unavailable to users or temporarily removing published data from the website. The Service will ensure that restriction is clearly indicated in the relevant system so the data isn't further processed, just stored.

The table below details when the obligation arises and the circumstances the restriction can be lifted.

Obligation to restrict personal data where;	**Circumstances restriction can be lifted;**
The data subject has disputed the accuracy of the data, and the Service is verifying accuracy.	The data subject has consented to further processing
The processing is unlawful but the data subject has opposed the erasure and requested restriction of its use instead	Establishment, exercise or defence of legal claims
The Service no longer requires the data but the data subject requires it to establish, exercise or defend legal claims	Protection of the rights of another living individual
The data subject has objected to processing and the Service are in the process of verification whether the objection is on legitimate grounds.	Reasons of important public interest

A data subject who obtained the restriction of processing shall be informed by the Service before the restriction of processing is lifted.

Where a restriction request has been upheld, the Service shall instruct third parties that have been sent personal data that the data subject has made a request for restriction. The exception to notifying third parties is if this proves impossible or involves disproportionate effort.

The Service shall inform the data subject of such third parties if they request this information.

RESPONSE TO TRANSFER (DATA PORTABILITY) REQUESTS

This right allows a data subject to obtain and reuse personal data for their own purposes across different services.

When requested by a data subject, the Service shall transmit personal data without hindrance, where:

- The data subject has provided it to the Service (this is provided knowingly and actively by the data subject as well as generated by the data subject's activity, e.g. fitness monitor)
- The processing of the data is based on consent or for the performance of a contract with the data subject, and

- The processing is carried out by automated means.

Transmitted data shall be in a structured, commonly used and machine-readable format.

If the above conditions are met, and it is technically feasible for the Service to achieve, the data subject can request the Service transmits its data to another organisation. The Service is not responsible for compliance of the receiving organisation with data protection law as it would be acting upon the data subjects' request.

As a safeguard the Service will ensure that the data to be transmitted are indeed those that the data subject wants to transmit and will take necessary security measures to ensure the data is transmitted securely.

If the data concerns other individuals, the Service will consider whether providing the information would prejudice the rights of those individuals and take the same approach detailed in the Response to Access section.

RESPONSE TO OBJECTION REQUESTS

A data subject can object to the processing of their personal data, including profiling, on grounds relating to their particular situation.

Where a request is received, the Service is under an obligation to act upon a request where one of the following conditions applies:

- The processing of the data is based on it being necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Service (statutory functions)
- The processing of the data is based on it being necessary for a legitimate interest pursued by the Service
- The Service is processing the data for purposes of scientific or historical research or statistical purposes
- The processing of the data is for direct marketing purposes

In regards to the first two bullet points (conditions), whilst the Service considers the request it will restrict further processing until it reaches a decision. The Service will issue a refusal notice to such request, where it can demonstrate that it:

Has compelling legitimate grounds which override the data subject's interests or their fundamental rights and freedoms, or; the data is required for the establishment, exercise of defence of legal claims.

In regards to the third bullet point (conditions), if the processing is necessary for reasons of public interest the Service is not required to comply with the objection.

If the processing is for direct marketing purposes the Service **will immediately cease** to process for such purpose.

EXCEPTIONS

The forthcoming Data Protection Act provides exemptions which enable the Service to dis-apply data subject rights in certain circumstances. For example, the prevention and detection of crime (e.g. benefit fraud) or disclosure required for legal proceedings / advice (e.g. obtaining legal advice in regards to a claim)

Where appropriate, the Service will take into consideration the relevant exemptions and where an exemption is applied the Service is not required to cite the exemption used.

REQUEST LOG

The **CAOSIT** are responsible for maintaining a log of requests, and associated documentation to ensure that the Service is able to track the amount of requests that it receives, that its response is compliant and that it is responding to those requests within the correct timeframe.

RETENTION

A copy of all the data retrieved must be taken for reference should the data be challenged by the data subject. These will be maintained in line with NYFRS's retention schedule and retained for 3 years, where challenged this will be retained for 6 years.

COMPLAINTS / APPEAL

If the data subject or their representative is not satisfied with the outcome of their rights request, in the first instance, the individual is encouraged to attend an informal meeting or have a discussion, with a view to addressing and resolving the issues locally with the **CAO Manager**.

- Writing to the correspondence address of the CAOSIT FAO CAO Manager,
- Phoning 01609 780150

Where the Data Subject would like to make a complaint regarding the rights request, they can submit a Complaints Form via our website:

http://www.northyorksfire.gov.uk/contact-us/complaints-compliments

You can also contact the DPO for further advice at:

Data Protection Officer
Veritau Ltd
County Hall
Northallerton
DL7 8AL

Tel: 01609 533219
E-mail: information.governance@veritau.co.uk

You can contact the Information Commissioner directly who is the statutory regulator for an assessment on how North Yorkshire Fire and Rescue Service processed your request.

The Information Commissioner can be contacted at:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow,
Cheshire, SK9 5AF

Tel: 01625 545 745

E-mail: casework@ico.org.uk

Website: www.ico.org.uk/concerns/

APPENDIX A – APPLICATION FORM FOR THE DATA SUBJECT

NORTH YORKSHIRE
FIRE & RESCUE SERVICE

DATA PROTECTION – RIGHTS REQUEST FORM

Please return this form by email to: **CAO.Serviceinformation@northyorksfire.gov.uk**

Or by post to: **CAO Service Information, North Yorkshire Fire & Rescue Service, HQ, Thurston Road, Northallerton, North Yorkshire, DL6 2ND**

You can phone: 01609 780150 to speak to someone about the request or make a request. Your request will be documented but won't be progressed until we have verified identification.

1. Are you the Data Subject? (the person to whom the data relates) (Circle one)	
Yes	If you are the Data Subject please complete Section 2 and supply a **photocopy** of 2 forms of evidence of your identity, such as Driving Licence and Utility Bill. (Please now go to Section 5).
No	Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed. (Please complete Sections 2, 3 and 4 then go to Section 5). **Children Data –** If you are making the request on behalf of your child, enclose a copy of the child's birth certificate or a copy of your proof of parental responsibility order.

2. Details of data subject (the person to whom the data relates)			
Name *:			
Address*:			
Post Code*			
Telephone Number		Mobile Number	
Email Address			

3. Details of person requesting the information (if different to Section 2)			
Name*:			
Name of Company (if applicable)*:			
Address*			
Post Code*			
Telephone Number		Mobile Number	
Email Address			

***Mandatory fields**
Optional fields will assist if we need to get in contact to discuss the application.

4. Relationship to the Data Subject	**Tick as appropriate**
Legal representative	
Power of Attorney	
Parent / Guardian / Carer	
Other (please specify below)	

Section 5:
You are now required to identify the right you wish to exercise. Please be aware that not all rights are absolute rights so in accordance with the law there will be occasions whereby a refusal notice is issued or exemptions applied.

Your right to withdraw consent from processing is only applicable where this is the basis being used to process your information.

5. Right you wish to request	**Tick the applicable one**		**Tick the applicable one**
Right of access		Right to data portability	
Right to rectification		Right to object	
Right to erasure		Right not to be subject to a decision based solely on automated processing, including profiling	
Right to restriction		Right to withdraw consent to processing	

Description Box:
Please be as clear as possible in making your request, providing as much detail as you can to help us understand your request and locate the information. For example, it may be helpful if you can refer to the dates and locations of events or meetings, the names of people you have spoken to before, the location of the information if known, the subject of any documents or emails, the names or authors of any messages or documents and any relevant time periods.

If we require you to be more specific about the information we will come back to you.

Warning - Attempting to obtain / alter personal data to which you are not entitled may be an offence under the General Data Protection Regulations

6. Declaration

I certify that the information given on this request form to North Yorkshire Fire and Rescue Service is true. I understand that it is necessary for North Yorkshire Fire and Rescue Service to confirm my/the Data Subject's identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Signature :		Date :	

Your Checklist:

Is your contact information correct?	
Have you signed the form?	
Have you enclosed acceptable identification and if applicable written authority from the data subject?	
Have you provided the necessary information to assist in identifying and finding the information?	

The information that you supply with your Request for Information will be entered into a filing system and will only be accessed by authorised persons of North Yorkshire Fire & Rescue Service. The information will be retained and will be used for the purpose of (a) processing your request; (b) helping us to make decisions about how we handle requests for information, and (c) informing the public from time to time of the types of requests we have received and how we have responded. In the case of (c), we will NOT publicise the identity of any individual who has made a request. All personal information will be held in accordance with the requirements of data protection laws.

APPENDIX B – DATA SUBJECT RIGHTS REQUEST CHECKLIST

Request Forwarding

- ☐ All staff must forward a personal data request to the **CAOSIT** for all requests received from members of the public or an employee.

CAOSIT / DATA PROTECTION OFFICER:

Identification Checklist

Check the identity of the data subject has been verified with acceptable proof of identification, including one of the following:

- ☐ Full valid driving licence;
- ☐ Birth certificate or certificate of registry of birth or adoption certificate;
- ☐ Full valid current passport;
  AND one of the following:
- ☐ Gas, electricity, water or telephone bill in the data subject's name for the last quarter.

  OR
- ☐ Power of attorney / proof of data subject consent / proof of guardianship etc.
- ☐ Confirmed with employee

Response Checklist for All Responses

Check that:

- ☐ The response doesn't conflict with any legal, regulatory or other such constraints (GDPR, DPA, HRA, Employment Law);
- ☐ Exceptions have been considered where necessary and redactions where appropriate
- ☐ A response has been provided without undue delay and in any event within one month of receipt of the request;
- ☐ The data is presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- ☐ The response is in the medium requested by the data subject. Where no medium has been specified, check the response is:
- ☐ In writing, for requests received in writing;
- ☐ In a commonly used electronic form by secure email (Egress), for requests received via email;
- ☐ Provided orally, for requests received orally.

Response Checklist for Data Access Requests

Check the response has included:

- ☐ The data requested;
- ☐ The purposes of the processing;
- ☐ The categories of personal data concerned;
- ☐ The recipients or categories of recipient to whom the personal data have been or will be disclosed (where transferred outside the EU, include the appropriate safeguards relating to the transfer);

- ☐ Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- ☐ The existence of the right to request from NYFRS the rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- ☐ The right to lodge a complaint with the ICO;
- ☐ Where the personal data are not collected from the data subject, any available information as to their source;
- ☐ Any existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Response Checklist for Data Rectification Requests
Check the response has included:

- ☐ Confirmation that the data has been updated (or added to via a supplementary statement) in all locations in which it resides;
- ☐ Confirmation that all the relevant third parties that have been sent the personal data have been informed that the data subject has made a rectification request and what the rectification request was;
- ☐ Right to be informed who the third parties are
- ☐ Confirmation from all the relevant third parties that have been sent the personal data that they confirm they have been informed by the Service that the data subject has made a rectification request.

Response Checklist for Data Erasure Requests
Check the response has included:

- ☐ Confirmation that the data has been securely erased in all locations in which it resides;
- ☐ Confirmation that all the relevant third parties that have been sent the personal data have been informed that the data subject has made a erasure request and what the erasure request was;
- ☐ Right to be informed who the third parties are
- ☐ Confirmation from all the relevant third parties that have been sent the personal data that they confirm they have been informed by the Service that the data subject has made an erasure request.

Response Checklist for Restriction Requests
Check the response has included:

- ☐ Confirmation that the data processing has been restricted/stopped for that specific purpose;
- ☐ Confirmation that all the relevant third parties that have been sent the personal data have been informed that the data subject has made a restriction request and what the restriction request was;
- ☐ Right to be informed who the third parties are
- ☐ confirmation from all the relevant third parties that have been sent the personal data that they confirm they have been informed by the Service that the data subject has made an restriction request;

- ☐ Confirmation that the data subject shall be informed by the Service before the restriction of processing is lifted.

Response Checklist for Data Transfer (Portability) Requests
Check that:

- ☐ The personal data was provided by the data subject
- ☐ The processing of the data is based on consent or contract;
- ☐ The processing of the data is carried out by automated means.
- ☐ Third parties information is protected

Check the response has included:

- ☐ Confirmation that the transfer has taken place;
- ☐ Confirmation that the transmitted data is in a structured, commonly used and machine-readable format.

Response Checklist for Objections Requests
Check that:

- ☐ The processing of the data is based on performance of a task carried out in the public interest or official authority, or;
- ☐ The processing of the data is based on a legitimate interest pursued by the Service
- ☐ The processing of the data is for the purposes of scientific or historical research or statistical purposes, or;
- ☐ The processing is for direct marketing purposes.
- ☐ First two conditions – restrict the data, whilst investigating
- ☐ If based on direct marketing – cease processing

Check the response has included:

- ☐ Confirmation of the outcome and the rationale