General Data Protection Regulation (GDPR)

Data Protection Policy

May 2018

Document Control

Related Documents

Title	Author	Version	Date

Revision History

Release Date	Revision	Version	Summary of Changes
22.05.2018	**0.1**	**0.1**	**Shared with members of GDPR Working Group for review on 24.05.2018**

Reviewed By

This document (or component parts) has been reviewed by the following:

Post/Group Title	Revision	Version	Approval Date
GDPR Working Group	**0.1**	**0.1**	

Introduction

Cumbria County Council supports the objectives of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) and seeks to ensure compliance with this data protection legislation.

The processing of data by the council is essential to services and functions, and will often involve the use of personal and/or 'special category' personal data. Compliance with the data protection legislation will ensure that such processing is carried out fairly and lawfully. An explanation of key terms can be found on InTouch at: http://www.intouch.ccc/gdpr/gdpr.asp

The GDPR and the Human Rights Act (1998) (HRA) Article 8, make it clear that the processing of personal data must respect the rights and freedoms of the data subject (individual), but at the same time be adequate enough for the council to function effectively.

This policy should not be read in isolation and regard should be given to other related council policies: http://www.intouch.ccc/security/infosec/default.asp

Purpose

The purpose of this policy is to ensure that the provisions of the GDPR and DPA are adhered to whilst protecting the rights and privacy of living individuals; ensuring their personal data is not processed without their knowledge.

In particular this policy will:

- assist the council to comply with all requirements of the GDPR and DPA;
- ensure that personal data is readily available on request and that requests from data subjects are dealt with in a timely manner;
- ensure adequate consideration is given to whether or not personal information should be disclosed;
- ensure increased awareness of data subjects to the amount of personal data processed and stored by the council about them and advise them of their rights under the data protection legislation.

The council will endeavour to promote greater openness, provide increased transparency of data processing and build public trust and confidence in the way that the council manages information about their customers.

Aims

This policy sets out the council's commitment to upholding the data protection principles set out in the GDPR and managing information held fairly and lawfully. It seeks to:

- strike an appropriate balance between the council's need to make use of personal information in order to manage their services efficiently and effectively whilst giving respect for the privacy of individuals;
- support council employees to meet their statutory obligations under the GDPR and DPA and provide a guide to the public on the council's' obligations with regard to the processing of their personal data.

Statement

This policy applies to the acquisition and processing of all personal data within the council and sets out how the council will ensure that individual rights and freedoms are protected.

- the council will comply with Article 8 of the HRA in respect of the processing of personal data;
- the council, as the Data Controller, will make individuals aware of the purpose(s) it is processing their personal data for and will seek consent where appropriate;
- 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- the council will manage breaches of the GDPR in accordance with the Data Breach Reporting Policy and Procedure;
- the council will provide general information to the public about their statutory rights under the GDPR and DPA on our website;
- the council will hold the minimum amount of personal data necessary to carry out its functions, and every effort will be made to ensure the accuracy and relevance of data processed.
- the council will keep all electronic and manual records in accordance with its Records Management Policy
- the personal data the council holds will be kept in accordance with the six principles of the GDPR and in line with the council's Retention and Disposal Schedule.
- periodically a risk assessment will be undertaken, via audit reviews, for all data processing, and when inadequate controls are identified, technical and organisational security measures will be taken, appropriate to the level of risk identified.
- personal data will only be used for the direct promotion or marketing of goods or services with the explicit consent of an individual.
- elected members and staff will be trained to an appropriate level in the use and supervision of personal data.
- breaches of this policy may be subject to action under the council's disciplinary procedure.

Principles

The council will abide by the six data protection principles as detailed below: Personal data shall be:

1) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) not be considered incompatible with the initial purposes ('purposed limitation')
3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy')

5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Roles and Responsibilities

The councils' Extended Leadership Team and GDPR Working Group is responsible for approving this policy and for managing compliance with the GDPR and DPA.

The council's Data Protection Officer is responsible for the provision of advice, guidance and training regarding data protection legislation and will be responsible for keeping this document up to date.

All employees of the council will be responsible for ensuring that Subject Access Requests are dealt with in accordance with this policy and that personal data is processed appropriately. This includes ensuring that personal data supplied to the council is accurate, up-to-date and held securely.

Heads of Service will be responsible for ensuring operational compliance with this policy within their own departments and for becoming involved in consultations with the Information Governance Manager when applicable.

Internal Audit will undertake reviews to assess the procedures and policies in place that relate to data protection.

Information Requests

Requests from data subjects for copies of personal data the council holds about them (Subject Access Requests) must be made in writing. This includes requests transmitted by electronic means, providing they are received in a legible form and are capable of being used for subsequent reference.

All Subject Access Requests should be emailed or scanned in and sent to the Information Governance Team at: information.governance@cumbria.gov.uk.

The Information Governance Team will:

- provide advice to assist individuals to formulate requests
- verify data subject identity where they are unknown to the council or have not used council services for a significant period
- seek additional clarification where the information sought is not described in a way that would enable the council to identify and locate the requested material, or the request is ambiguous
- seek evidence of consent from an individual where a third party has requested access to their personal data

Timescales and Extensions

The council is committed to dealing with requests for information promptly and no later than the statutory guideline of one calendar month.

The council would not expect every application for information to take one calendar month and will endeavour, where possible, to provide the requested information at the earliest opportunity from the date of the request.

However, if the council considers the request to be complex, they may extend the time by up to two extra calendar months.

In this instance the council will notify the applicant in writing that the SAR requires further time and will provide an estimate of a 'reasonable time' by which they expect a response to be made.

These estimates shall be realistic and reasonable taking into account the circumstances of each particular case.

Data Subject Rights

As well as access rights data subjects also have the rights below:

Right to be informed	The Council has to be more transparent and, therefore, more accountable on using personal information. This means that privacy notices are be reviewed and updated across all Council directorates.
Right of access	The new DPA expands the individual right to access personal data and supplementary information. This is called a Subject Access Request (SAR). The deadline for compliance is reduced from 40 days to one month.
Right to rectification	The new DPA also has the right to have personal data rectified if it is inaccurate or incomplete.
Right to erasure (or 'right to be forgotten')	An individual can ask an organisation to delete or remove their personal information where there is no compelling reason for its continued processing. The organisation has to explain if it can or cannot comply. If the Council collects information by statutory authority, this will amount to a good reason to retain the information. The process protects against those trying to delete or destroy data they are not entitled to have removed.
Right to restrict processing	Individuals have a right to 'block' or suppress processing of personal data depending on whether the information is collected by statute or consent. When processing is restricted, the Council can store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.

Right to data portability	In specific situations, an individual can request that an organisation provide a copy of their personal data in a format that they can take to another provider. This is rare in local government as it relies on automated processing in which no person is involved in the processing such as a Fitbit recording someone's exercise and transmitting it to a service provider.
Right to object	The individual can object to processing in three areas and an organisation needs to have the process in place to respond to these objections. 1. Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling). This means processing where it is done in the public interest and the individual disagrees that the public interest has been assessed correctly. 2. Direct marketing (including profiling) means that any direct marketing the Council does must stop if an individual objects. 3. Processing for purposes of scientific/historical research and statistics. In certain circumstances, an individual can object to having their personal data included in some scientific/historical research and statistics.

Further information on council processes and procedures can be found at: http://www.cumbria.gov.uk/council-democracy/accesstoinformation/dataprotection/default.asp

Exemptions

The GDPR is designed to prevent access by third parties to a data subject's personal data. However, under the DPA there are circumstances which allow disclosure of a data subject's personal data to a third party, or for it to be used in a situation that would normally be considered to breach the GDPR.

Exemptions from the non-disclosure of personal data are given below. This list is not exhaustive.

- Crime and taxation: general
  - the prevention and detection of crime
  - the apprehension or prosecution of offenders, or
  - the assessment or collection of any tax or duty or of any imposition of a similar nature
- Crime and taxation: risk assessment systems
  - Immigration
  - Information required to be disclosed by law etc. or in connection with legal proceedings

The council will only use these exemptions where it is in the public interest to do so, i.e. prevention of crime, or where the functioning of the council requires the processing of personal information to be exempt so that it can provide statutory services to members of the public.

Refusing Requests

The council will not supply information to a data subject if:

- the Subject Access Request (SAR) has not been made in writing;
- the identity of the data subject cannot be identified;
- responding to the request will inadvertently disclose personal information relating to another individual without their consent;
- the same or similar information has been requested within the last 3 months (dependent on nature of data)

The council considers that when a valid reason, which is both robust and legally defendable, exists for refusing the disclosure of information to either the data subject or a third party, the information should be withheld.

When information is withheld, full explanations of the reasoning behind the refusal must be provided to the applicant. This explanation must also include the details of how the applicant can complain about the council's decision.

All requests for personal data made by the data subject will be dealt with under Chapter 3 - Rights of the Data Subject section of the GDPR, not the Freedom of Information Act 2000.

Data Breaches

The General Data Protection Regulation (GDPR) comes into force in May 2018 and places a duty on the council to report certain types of personal data breaches to a supervisory authority - the Information Commissioner. When a personal data breach happens and is likely to affect individuals' rights and freedoms, the council will:

- report it to the Information Commissioner (ICO) within 72 hours of becoming aware of it (where possible)
- tell the individual immediately

The council has updated its breach detection, investigation and internal reporting procedures to reflect the changes in the law and will keep a record of all personal data breaches, whether they are reportable or not. Further information can be found at: http://www.intouch.ccc/gdpr/gdpr.asp

Appeals and Complaints

Where an applicant is dissatisfied with the level of service they have received, they are entitled to complain about the actions of the council through the Internal Review Procedure.

Further details can be found at: http://www.cumbria.gov.uk/council-democracy/accesstoinformation/internalreviewscomplaints.asp

The applicant will receive a response to their correspondence within twenty working days.

If the applicant remains dissatisfied with the council's reply, they have the option of taking their complaint to the Information Commissioner (at the address below) who will independently adjudicate each case and make a final decision.

Post: Information Commissioner's Office Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF
E-mail: casework@ico.org.uk

Telephone: 01625 545700