Epping Forest District Council

Data Protection

Protocol for the disclosure of personal data pursuant to Section 29(3) of the Data Protection Act 1998

1. INTRODUCTION

1.1 Epping Forest District Council is a data controller pursuant to the Data Protection Act 1998 ('the Act'). The Council regards the fair and lawful treatment of personal data as important to the efficient performance of its operations and the delivery of services, and to maintaining confidence between the authority and those with whom it works. The Council fully endorses and adheres to the principles of data protection set out in the Act.

1.2 The Act contains a number of exemptions to the fair processing and non-disclosure provisions, whereby it would not normally be lawful for the Council to disclose personal data to a third-party, without consent. The Council receives regular requests for the disclosure or 'sharing' of personal data relating to identifiable individuals, that seek to apply these exemptions. This Code of Practice has been developed specifically in relation to Section 29(3) of the Act, to provide a framework for ensuring that all requests that claim this particular exemption are treated in a lawful and consistent manner.

1.3 Data sharing requests pursuant to Section 29(3) of the Act are made for the disclosure of relevant information in connection with the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of tax. Whilst in many cases it is likely to be in the public interest for the Council to assist investigatory organisations by providing the information sought by such requests, the authority is committed to ensuring that all disclosures of personal data are fair, and comply fully with the provisions of the Act.

1.4 This protocol seeks to minimise the risk of a breach of data protection legislation and principles in the Council's handling of relevant data sharing requests, which could present a significant financial and reputational risk to the authority. The protocol applies only to data sharing requests made in relation to crime and taxation related maters, and does not affect the operation of existing information sharing agreements currently in place between the Council and relevant organisations. The protocol similarly does not apply in 'gateway' circumstances where the Council is legally obliged to share particular personal data with a named organisation, or is expressly permitted to disclose information for certain purposes (such as the administration of Housing Benefit and Council Tax Benefit).

1.5 Separate protocols are in place for other exemptions to the provisions of the Act, and for the Councils approach to Subject Access Requests.

2. DATA PROTECTION PRINCIPLES

2.1 Personal data is defined by the Act as biographical information relating to a living individual, who can be identified either from the data alone, or from the data in conjunction with additional data held by, or likely to come into the possession of, the data controller. A data controller is the person (or organisation) who determines how personal data is to be processed. In the case of personal data held by the Council, the authority itself is the data controller.

2.2 The Act requires a data controller to comply with eight Data Protection Principles, the first of which requires that personal data must be processed 'fairly and lawfully'. The act of 'processing' personal information concerns (amongst other operations) the organising, retrieving, consulting, using, adapting, altering or deleting of data, and is therefore virtually limitless in scope.

2.3 The Act stipulates that in order for processing to be fair, an individual who is the subject of the personal data to be processed (the 'data subject'), must be provided with details of the purposes for which that processing will take place, together with any other information that is relevant in the specific circumstances. This is known as fair processing information.

2.4 The term ‘data sharing’ in the context of the Act, means the disclosure of personal data and information from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Whilst data sharing is usually taken to mean the sharing of sharing data between different organisations, the data protection principles of the Act also apply to the sharing of information within the Council, and its approach to data sharing therefore applies equally to both ‘external’ and ‘internal’ sharing requests.

3. DATA PROTECTION ACT 1998 - SECTION 29

3.1 Section 29 contains categories of exemption from some of the provisions of the Act, which are referred to as the ‘crime and taxation purposes’. These purposes are:

(a) the prevention or detection of crime;
(b) the apprehension or prosecution of offenders; or
(c) the assessment or collection of any tax or duty or of any imposition of a similar nature.

3.2 The third crime and taxation exemption (Section 29(3)) provides that personal data is exempt from the non-disclosure provisions in any case where the disclosure is required for any of the crime and taxation purposes, and where the application of those provisions in relation to the disclosure would be likely to prejudice (i.e. significantly harm) any of the crime and taxation purposes. This exemption is not a blanket or automatic exemption, and must be applied by the data controller on a case by case basis.

3.3 Section 29(3) of the Act provides an exemption from the requirement to provide fair processing information to a data subject, where processing is necessary for the crime and taxation purposes. The exemption is only applicable to the extent that the provision of fair processing information would prejudice the purpose for which the personal data is required to be shared.

3.4 The Section 29(3) exemption allows a data controller to disclose relevant personal information to a third-party in connection with crime and taxation related purposes, which in normal circumstances might represent a breach of the Act. Section 29(3) requests are usually made by the police and other organisations that have an obvious crime prevention or law enforcement function, such as HM Revenue and Customs, the Border Agency, the Department for Work and Pensions, or the benefit fraud activities of local authorities. In reality however, data sharing requests could be made by a wide variety of organisations and agencies that might seek to apply the exemption.

3.5 Section 29(3) of the Act does not automatically permit the disclosure of all personal information in all circumstances. The exemption only allows a data controller to release personal information for stated purposes, and then only if non-disclosure would be likely to prejudice an attempt by the requesting organisation to prevent or investigate a crime, apprehend or prosecute offenders, or assess or collect tax or duty.

3.6 Although the Section 29(3) exemption permits the disclosure of personal data where necessary in connection with one of the specified crime and taxation purposes, it is entirely at the discretion of data controller as to whether it provides a substantive response to a request for the disclosure of personal data, unless it is required to do so by law (i.e. where there is a statutory obligation to disclose or the authority is served with a court order compelling disclosure). It is for the data controller to determine whether the non-disclosure of requested personal data would prejudice any of the crime and taxation purposes. A data controller may, if it has concerns about the disclosure of personal information, ask the investigating organisation to secure a court order requiring the release of the personal information.

3.7 Section 29(3) of the Act does not require a data controller to disclose personal information in response to a data sharing request, but merely provides an exemption for the release of relevant information without the consent of the data subject, in particular circumstances. A data controller would not be in breach of the Act if it declined to disclose personal data in response to a request, or if it disclosed relevant information in response to a court order.

4. DATA SHARING REQUESTS - RESPONSIBILITY AND PROCESS

4.1 The Council's designated Data Protection Officer is responsible for considering and responding to requests for the disclosure of personal information pursuant to Section 29(3) of the Act, including the processing of requests and the disclosure (or otherwise) of appropriate personal data. All data sharing requests must be made directly to the Data Protection Officer, and not to any other officer or service of the Council.

4.2 All requests for the disclosure of personal data in accordance with the Section 29(3) exemption, must be made in writing. The Council will not accept any request made orally or by telephone. All such data sharing requests must:

(a) be submitted on the headed paper of the organisation requesting the personal data;
(b) state the section of the Act under which the request is made, together with any other statutory basis for disclosure that is considered to apply (if appropriate);
(c) specify in as much detail as possible, the type and nature of the personal data that is sought;
(d) state, in as much detail as possible in the particular circumstances, the purpose(s) for which the personal data is required;
(e) state (if it is the case) whether a failure to disclose the required personal data would prejudice the purpose(s) for which the information is requested; and
(f) be signed by the requestor and be countersigned by an appropriate supervisor, and provide the names, positions and full contact details of both, including addresses, telephone numbers and secure (GCSX, PNN, GSI etc.) e-mail addresses.

4.3 Where requests are made by the police, the relevant force's 'Personal Data Request Form', based on the template set out in the Association of Chief Police Officers' Data Protection Manual of Guidance (external link), may be submitted in place of a letter of request. The form must be completed in accordance with each force's own requirements, and as fully as necessary in the circumstances of the particular enquiry. The format of internal data sharing requests must reflect the template 'Data Request Declaration Form', which is available from the Data Protection Officer.

4.4 It is recognised that the nature and potential urgency of crime and taxation related investigations may be such that it is appropriate for requests to be made by e-mail. In such circumstances, the request must still be provided in the format prescribed in Section 4.2 above (including signatures), but can be submitted as a scanned file. Data sharing requests made by email must use a secure (GCSX, PNN, GSI etc.) network, and the e-mail address of the requesting organisation must be readily verifiable as belonging to that organisation. Wherever possible, the Data Protection Officer will verify the authenticity of the email address provided.

4.5 Incomplete data sharing requests, or those that do not satisfy the requirements set out in Sections 4.2 to 4.4 above, will be rejected and will not be considered by the Council. Requests that do not specify (if appropriate) that failure to disclose the requested personal data would prejudice the purpose(s) for which the data is required, will similarly not be accepted by the Council in any circumstances, as these will not meet the criteria for the Section 29(3) exemption. This confirmation is not required in circumstances where the Council may be legally obliged to share particular personal data, or is expressly permitted to disclose information for certain purposes, although the statutory basis for disclosure must be specified in the data sharing request.

4.6 For every valid request for the disclosure of personal information (and concerning each separate data subject), the Data Protection Officer will consider the following matters:

(a) is the organisation requesting the personal information who they say they are?
(b) is the personal information required for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of tax or duty?
(c) has the organisation requesting the personal information cited legislation (other than the Data Protection Act) which gives a statutory right of access to the data?
(d) is it necessary for the Council to provide the requested personal data, or can the information be obtained from another source?
(e) how will the requested personal information assist the prevention or detection of a crime? and
(f) if the Council does not release the personal information, will this significantly harm the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of tax or duty.

4.7 The risk to be assessed by the Data Protection Officer in connection with Section 4.6(f) above, is that it must be highly likely that an investigation will be impeded, given the circumstances of the particular case. In practice, it is unlikely that the Data Protection Officer will have sufficient information with which to make such judgement, and reliance will therefore be placed on the confirmation of the requesting organisation that non-disclosure would prejudice the purpose(s) for which the data is required.

4.8 In circumstances where the Council is legally obliged to share particular personal data with a named organisation, or is specifically permitted to disclose information for certain purposes, it is not necessary for the requesting organisation to state whether failure to disclose the requested personal data would prejudice the purpose(s) for which the information is requested.

4.9 If, having considered each of the matters at Section 4.6(f) above, the Data Protection Officer considers that personal data should not be disclosed or only disclosed in part, the investigating organisation will be advised of the reasons pertaining to the particular case. The investigating organisation may seek a court order for the release of the personal information, or a review of the decision of the Data Protection Officer through the Council's Compliments and Complaints scheme. Alternatively, the investigating organisation may request the Information Commissioner's Office (ICO) (external link) to undertake a review of the way that the Council has dealt with the request, and the disclosure (or not) of relevant personal data.

4.10 Upon receipt of a written request satisfying the requirements of Section 4.2 above, the Data Protection Officer will seek the requested data from the Council's service area records and databases as appropriate, through nominated directorate data protection representatives. Following collation of the required data (if available), the Data Protection Officer will make a judgment as to whether:

(a) disclosure of any or all of the required data is necessary for the purposes for which it has been requested; and
(b) notification of the data subject of any intended disclosure would prejudice the stated purposes.

4.11 In responding to the data sharing request, relevant personal data will only be disclosed to the extent that the criteria set out at Section 4.10(a) above are satisfied.

4.12 Whilst it is good practice for a data controller to tell a data subject as soon as possible after the risk of prejudice has passed, that personal information about them has been shared, this will not usually be practicable, as the Council will be unaware of the progress or outcome of

an investigation. As it is unlikely that the Data Protection Officer will have sufficient information to make such judgement, reliance will again be placed on the original confirmation of the requesting organisation that non-disclosure would prejudice the purpose(s) for which the data was required. Notification of the disclosure to the data subject will be undertaken wherever information is available to demonstrate that the risk of prejudice has passed

4.13 Following a release of personal data by the Council, the recipient organisation would become the data controller in respect of the information disclosed. All responses to data sharing requests will therefore advise that the personal information provided by the Council in response to the request, must:

(a) not be used for any purpose other than that for which it has been provided;
(b) be managed in accordance with the Data Protection Act 1998 and any other relevant provisions; and
(c) only be retained whilst the purpose for which it has been supplied continues to exist.

4.14 All decisions to share (or withhold) personal data pursuant to a Section 29(3) of the Act will be fully and completely documented, including the reasons for each such decision, particularly as disclosure is made without the consent of the data subject. The Data Protection Officer will therefore complete a 'Data Sharing Decision Record' for every Section 29(3) request, retaining in all cases:

(a) the original data sharing request and any subsequent correspondence;
(b) any draft response and amendments to the request (where relevant);
(c) a copy of the final decision and response to the request, including any personal data disclosed; and
(d) the reasons for each such decision, including justification for the non-disclosure of personal information (if appropriate).

4.15 The recording of the decision of the Data Protection Officer in respect of each data sharing request is important, in case a challenge is made to the Council's disclosure (or withholding) of personal information. This could be in the form of a complaint to the authority or the ICO, or through a claim for compensation in the courts, and the record will be of assistance if it is subsequently necessary to justify the authority's response to the request, or if a further similar data sharing request is received.

5. SUPPLY OF PERSONAL DATA

5.1 The seventh data protection principle requires that appropriate technical and organisational measures be taken against unauthorised or unlawful disclosure of personal data. Accordingly, the Council must ensure that the arrangements by which personal data is disclosed are appropriately secure, given the nature of the data concerned in any particular circumstance.

5.2 The Council's preferred method for the provision of personal data, is by collection from the Civic Offices. Disclosure in person will be made where an appointment for collection has been arranged with the Data Protection Officer, and the collecting individual's warrant card/photographic identity card (or equivalent) is produced for inspection. In these circumstances, the collecting individual will be required to sign and date a 'receipt' for the completed response to the data sharing request, a copy of which will be retained by the Data Protection Officer.

5.3 Whilst e-mail is not a totally secure method of communication, it is recognised that the nature and potential urgency of crime and taxation related investigations may be such that it is appropriate for requests to be responded to by e-mail. In such circumstances, personal data

will only be transmitted through the secure GCSX email network, which enables the Council to interact and share data privately and securely with other public-sector organisations

5.4 Personal data will only be sent through the normal post at the discretion of the Data Protection Officer, and where specifically required by the requesting organisation. Where necessary, a recorded delivery service will be utilised. The disclosure of personal data will not be made by the Council by telephone or facsimile transmission, in any circumstances.

6. DATA PROTECTION OFFICER

6.1 The Council's designated Data Protection Officer can be contacted as follows:

Data Protection Officer,
Epping Forest District Council,
Governance Directorate,
Civic Offices,
High Street,
Epping,
Essex,
CM16 4BZ.

☎ (01992) 564180
✉ performance@eppingforestdc.gov.uk

6.2 The Data Protection Officer can also be contacted by secure email at:

GCSX: stautz@eppingforestdc.gcsx.gov.uk

7. DOCUMENT HISTORY

7.1 The Data Protection Officer is responsible for the maintenance of this protocol. The effectiveness of the protocol will be reviewed after relevant legislative changes, new case law, or revised guidance published by the ICO.

Prepared/Revised	Written by	Agreed/Authorised	Details of Change(s)
July 2013	S. Tautz (Data Protection Officer)	Corporate Governance Group (2/8/13)	Initial release of protocol. Published to website and intranet.
April 2014	S. Tautz (Data Protection Officer)	S. Tautz (Data Protection Officer)	Protocol updated as required to reflect new senior management structure. Republished to intranet and website.