Requests for personal data about public authority employees

Freedom of Information Act
Environmental Information Regulations

Contents

Overview 3
What the legislation says 4
Personal data about employees 5
Requests for information about your employees 5
Special category personal data 6
Criminal offence data 7
Article 6 lawful basis for processing 8
  Lawful basis (a) - consent 8
  Lawful basis (f) – legitimate interests 9
Balancing test – some key questions regarding the personal data of public authority employees 10
  1. What potential harm or distress may disclosure cause? 10
  2. What are the reasonable expectations of the individual? 11
  3. Does the legitimate interest outweigh the interests and rights of the individual? 13
Types of information 14
  Salaries and bonuses 15
  Termination of employment 16
  Lists, directories and organisation charts 17
  Job descriptions 18
  Names in documents 18
  Registers of interests 19
  Disciplinary files 20
  Representatives of other organisations 20
Good practice 21
More information 21

Introduction

The Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) give the public rights to access information held by public authorities.

An overview of the main provisions of FOIA and the EIR can be found in The Guide to Freedom of Information and The Guide to the Environmental Information Regulations.

This is part of a series of guidance, which goes into more detail than the guides, to help public authorities to fully understand their obligations and promote good practice.

This guidance explains in more detail how to apply FOIA exemptions and EIR exceptions relating to personal data. It therefore refers to the processing of personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). It is a guide to our general recommended approach, although decisions will always be made on a case by case basis.

The DPA and UK GDPR set out the UK data protection regime. The DPA also sets out separate data protection rules for the processing of personal data by competent authorities[1] for law enforcement purposes (DPA Part 3); and for processing by the intelligence services (DPA Part 4). For more information see our Guide to Data Protection.

This guidance is based on precedents established under the Data Protection Act 1998 (DPA98). It will be regularly reviewed and kept in line with new decisions of the Information Commissioner, tribunals and courts. Additional guidance is available on our guidance pages.

[1] A competent authority for the purposes of law enforcement means a person specified in Schedule 7 of the DPA and any other person if, and to the extent that, the person has statutory functions to exercise public authority or public powers for the law enforcement purposes.

Overview

- When you receive a request for information that constitutes personal data about your employees, in most cases you must decide whether disclosure would contravene the UK GDPR data protection principles. This usually involves considering whether disclosure would contravene principle (a) which requires the processing of personal data to be lawful, fair and transparent.

- In order for the disclosure to be lawful, it must satisfy one of the UK GDPR Article 6 lawful bases for processing. In most circumstances, the legitimate interests lawful basis is the most relevant.

- If the data is special category data, you also need a UK GDPR Article 9 condition for processing.

- In addition, you need to meet the requirements of Article 10 of the UK GDPR, if the data relates to criminal convictions and offences, including the alleged commission of offences and related proceedings.

- This applies to various types of employee information, including:
    - salaries and bonuses;
    - information about termination of employment and compromise agreements;
    - lists and directories of staff;
    - names in documents;
    - registers of interests;
    - disciplinary files; and
    - representatives of other organisations

- If an employee requests their own personal data, this information is exempt under FOIA and under the EIR there is no obligation to make it available. You should instead handle the request as a data protection subject access request.

- Personal data may also be exempt under FOIA or the EIR if:

    - disclosure would contravene an objection to processing; or
    - it would be exempt from a subject access request; and
    - the public interest favours withholding the information.

- There are also exemptions from the duty to confirm or deny whether you hold the requested information.

What the legislation says

Section 40 of FOIA provides an exemption from the right to information if it is personal data as defined in the DPA.

The EIR contains an equivalent exception. This is set out in regulations 5(3), 12(3) and 13.

These state that you should not disclose information under FOIA or the EIR if:

- it is the personal data of the requestor; or
- it is the personal data of someone else; and
    - disclosure would contravene the data protection principles;
    - disclosure would contravene an objection to processing; or
    - the data is exempt from the right of subject access.

FOIA section 40(1) and the EIR regulation 5(3) apply when the requester is asking for personal data about themselves. You should deal with these requests as data protection subject access requests. Further information is available in our UK GDPR guidance Right of access and in our law enforcement guidance The right of access.

There are separate provisions about the duty to confirm or deny whether you hold the requested information. Further information is provided in our guidance Neither confirm nor deny in relation to personal data.

In most cases, you should consider whether disclosure of third party personal data contravenes the UK GDPR data protection principles. This guidance focuses on how this exemption relates to information about public authority employees.

Our guidance on personal information explains how FOIA section 40 works in general terms and you should refer to this for further detail.

Personal data about employees

Requests for information about your staff can cover a wide range of topics, including the names of staff, organisation charts and internal directories, as well as other data which can identify individual employees. This can include information on:

- salaries and pensions;
- severance payments and compromise agreements;
- disciplinary or grievance cases;
- sickness statistics; and
- training records.

There is a further explanation of the definition of personal data in our Guide to the UK GDPR: What is personal data?

Requests for information about your employees

When you receive a third party request for personal data about your employees, you should usually consider whether it contravenes any of the data protection principles to disclose it. If so, the data is exempt under section 40(2) and section 40(3A).

The principle most likely to be relevant is principle (a) which states that processing must be lawful, fair and transparent.

Therefore, in order to decide whether disclosure contravenes principle (a) you need to determine:

- **Is disclosure lawful?**

    1. Is the information special category data?
    2. Is the information criminal offence data?
    3. Is there any Article 6 lawful basis for processing the personal data?
    4. Does lawful basis (a) (consent) apply?
    5. Does lawful basis (f) (legitimate interests) apply?
    6. Is disclosure generally lawful?

- **Is disclosure fair and transparent?**

There are a number of specific considerations which are relevant to the kind of information you are likely to hold about your employees.

Special category personal data

If the information is special category personal data, as defined in the UK GDPR, you need a UK GDPR Article 9 condition for processing, as well as an Article 6 basis for processing.

Special category data is defined in Article 9 of the UK GDPR:

> 'Special category data' is personal data about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes); health, sex life or sexual orientation.

This does not include criminal offence data which is treated separately.

Due to its sensitivity, the conditions for processing special category data are very restrictive and generally concern specific, stated purposes. Consequently, only two are relevant to allow you to lawfully disclose under FOIA or the EIR. These are in Article 9(2) of the UK GDPR:

- explicit consent; or
- the processing relates to personal data which has clearly been made public by the individual concerned.

When you are responding to a request for special category data about public sector employees, you are unlikely to be able to meet the requirements of the above conditions.

Such a request typically relates to the most personal aspects of employees' lives, for example their health or sexual life, rather than their working life. The employee is unlikely to have made this public and they are unlikely to give their consent for you to provide this data.

However, if they have made this information public, then you may be able to use the second condition above as your Article 9 condition for processing. For example, a request concerns details of trade union membership and an employee has made it publicly known that they are a member of a trade union.

Note that for special category data, consent for disclosure must be explicit consent. All consent must be freely given, which means giving people genuine ongoing choice and control over how you use their data. However explicit consent must also be expressly confirmed in words, rather than by any other positive action.

As a public authority in a position of power over your employees, you should avoid relying on consent unless you are confident you can demonstrate it is freely given.

Remember you may ask for consent for disclosure from the employee(s) in question, but you are under no obligation to do so. See below for a further discussion on consent and our UK GDPR guidance to consent.

For further information, please also see the guidance on Special category data.

Criminal offence data

Article 10 of the UK GDPR gives separate safeguards for personal data about criminal convictions and offences or related security measures.

Section 11(2) of the DPA adds the following personal data to this definition:

- the alleged commission of offences by the data subject; and
- proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

This is collectively referred to as criminal offence data.

In order to disclose criminal offence data lawfully, you must have an Article 6 basis for processing and in addition you must meet the requirements of UK GDPR Article 10.

This states that the disclosure must either:

- be carried out under the control of official authority; or
- meet a specific condition in Schedule 1 of the DPA.

Processing under the control of official authority does not apply in this context. Therefore, to consider the disclosure under FOIA or the EIR, you need to decide whether any of the conditions in Schedule 1 of the DPA apply. For further information, please see the guidance on Criminal Offence Data.

Due to its sensitivity, the conditions for processing criminal offence data are very restrictive and generally concern specific, stated purposes. Consequently, only two are relevant to allow you to lawfully disclose under FOIA or the EIR. They are similar to those identified above for special category data:

- consent from the data subject; or
- the processing relates to personal data which has clearly been made public by the individual concerned.

As with special category data, you are unlikely to be able to meet the requirements of the above conditions. In such circumstances, you must not disclose the requested information.

Article 6 lawful basis for processing

In all circumstances, you must have an Article 6 lawful basis for processing. For further information, please see our guidance: Lawful basis for processing and personal information.

There are six lawful bases for processing in Article 6, but only (a) consent or (f) legitimate interests are relevant to disclosure under FOIA or the EIR.

Lawful basis (a) - consent

You are under no obligation to ask your employees if they consent to the disclosure under FOIA or the EIR.

In novel or contentious situations it may be helpful for you to seek their views, but this only helps you to make your own decision about whether you should disclose. You may decide you can disclose on the lawful basis of consent, or you may consider the provision or refusal of consent as part of your legitimate interests balancing test.

However, it is not necessary to have the employee's consent in order to release the data. Consent is only one of the possible conditions for disclosure and if consent is not given, the disclosure may still satisfy the legitimate interests basis for processing.

It is important to note that consent must be a true indication of the employee's wishes. It must be a genuine choice, without any element of coercion. Furthermore, your employee must understand the implications of what they are consenting to, in particular that personal data about them will be disclosed not just to the requester, but to the world at large. If your employee has given their consent to the information being disclosed in these terms, then the condition is satisfied. For further detail, see our UK GDPR guidance to consent.

If your employee specifically objects to the potential disclosure at the time of the information request, then any concerns they have expressed may be relevant to the legitimate interests considerations and the judgement as to whether disclosure would be an unwarranted interference with their rights and freedoms. Please see our guidance on personal information for more information regarding the section 40 and the right to object.

Lawful basis (f) – legitimate interests

Without consent, legitimate interests - lawful basis (f) - is likely to be the most relevant basis for disclosure in response to an FOI or EIR request.

Under the UK GDPR, as a public authority, you cannot rely on legitimate interests as a lawful basis for any processing you do to perform your public authority tasks. However, for the purpose of considering the potential disclosure of information under FOIA or the EIR, you can do so.

This is because section 40(8) of FOIA, and regulation 13(6) of the EIR, confirm that for the purposes of considering disclosure, a public authority may consider the legitimate interests lawful basis for processing.

Article 6(1)(f) provides a basis for processing if it is:

> "… necessary for the purposes of legitimate interests pursued by the controller or by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child".

In order to assess whether this lawful basis is engaged you need to consider three key questions:

(i) **Purpose:** what is the legitimate interest in the disclosure of the information?

(ii) **Necessity:** is disclosure necessary for that purpose?

(iii) **Balancing test:** does the legitimate interest outweigh the interests and rights of the individual?

Please see our UK GDPR guidance on Legitimate interests. The guidance on personal information also discusses these points in detail, and outlines questions which you should consider. These questions are not all given here. However with respect to the balancing test, there are some key questions which are particularly relevant to public sector employees.

Balancing test – some key questions regarding the personal data of public authority employees

1. What potential harm or distress may disclosure cause?

You must consider the likely consequences of disclosure in each case. Personal information must not be used in ways that has unjustified adverse effects on the employee concerned.

Although your employee may regard the disclosure of personal information about them as an intrusion into their privacy, often this may not be a persuasive factor on its own, particularly if the information is about their public role rather than their private life.

You must be able to argue that adverse consequences would result from disclosure of the personal data. You must show that there is a connection between the disclosure of the requested information and the adverse consequences. For example, you have a strong argument for refusing a subsequent disclosure, if a previous disclosure of similar information has led to the targeting of individuals.[2]

You must therefore consider the nature of the information and judge the level of distress or damage likely to be caused. The greater this is, the more likely that the interests of the employee will override any legitimate interests in disclosure.

[2] Decision notice FS50401773

2. What are the reasonable expectations of the individual?

When considering the balancing test, it is important for you to take account of whether the proposed disclosure is within the employee's reasonable expectations.

You need to take into account both the expectations of the employee at the time their data was collected and their expectations at the time of the request, as this may have changed in the intervening period.

Considering the factors outlined in this guidance and in our guidance on personal information will help you to assess whether your employee could reasonably expect you to withhold their data in any particular case. Their expectations will depend on a number of factors, including:

- **Public v private life**

  Information about an employee's actions or decisions in carrying out their job is still their personal data. However, given the need for accountability and transparency about public authorities, there must be some expectation of disclosure.

  On the other hand, information that may be held in a personnel file about their health or disciplinary record, or payroll information about their tax code, all relates to them as individuals and to their personal circumstances. There is a greater expectation that you do not disclose such information.

- **Seniority**

  It is reasonable to expect that you disclose more information about senior public authority employees than more junior ones. Senior employees should expect their posts to carry a greater level of accountability, since they are likely to be responsible for major policy decisions and the expenditure of public funds. For example, a junior employee who is not accountable for their submissions to a senior government minister has no expectation that their name will be disclosed in response to an FOI request.[3]

  However, the terms 'senior' and 'junior' are relative. It is not possible to set an absolute level across the public sector below which personal information is not released. It is always

[3] Decision notice, paragraph 45 FER0409841

necessary to consider the nature of the information and the responsibilities of the employee in question.[4]

- **Public facing roles**

  It may also be fair to release more information about employees who are not senior managers but who represent your organisation to the outside world, as a spokesperson or at meetings with other bodies. This implies that the employee has some responsibility for explaining the policies or actions of your organisation. However, it does not apply simply because an employee deals with enquiries from the public or sends out material produced by others.[5]

- **Existing policy or standard practice of the public authority**

  Current government policy is to promote greater transparency throughout the public sector by more proactive publication of information. This has a bearing on what information employees may reasonably expect you to disclose.

  Furthermore, if you have a policy on the disclosure of personal information and have publicised this to your staff, this also affects their expectations.

  However the policy alone cannot determine whether the disclosure is reasonable in all circumstances. The issue is not simply whether an employee has an expectation that their personal data is not disclosed, but whether that expectation is a reasonable one to hold.

- **Privacy notices**

  The privacy notices you provide to your employees also help to shape their expectations. You should make it clear in a privacy notice that you may receive FOI and EIR requests for third party personal data and in most cases will consider whether disclosure would contravene principle (a) of the UK GDPR.

  The notice should make it clear that you have a legal obligation to process any personal data you hold when considering requests under these laws.

[4] First-tier Tribunal, paragraph 40 EA/2010/0060
[5] First-tier Tribunal EA/2011/0104

3. Does the legitimate interest outweigh the interests and rights of the individual?

Even though disclosure may cause distress to the employee, and they may have a reasonable expectation that you won't disclose their personal data, this does not necessarily mean that you should not disclose it. You must consider the legitimate public interest in disclosure and balance this against the rights of employees.

The data protection exercise of balancing the rights and freedoms of the employees against the legitimate interest in disclosure is different to the public interest test that is required for the qualified exemptions listed in section 2(3) of FOIA.

In the FOI public interest test, there is an assumption in favour of disclosure because you must disclose the information unless the public interest in maintaining the exemption outweighs the public interest in disclosure.

In the case of section 40(2), the interaction with the DPA means the assumption is reversed and a justification is needed for disclosure.[6]

The disclosure must not cause an unwarranted interference with the employees' rights. This means that you should follow a proportionate approach. You may be able to meet the identified legitimate interest by disclosing some of the information, rather than all the detail that the requester has asked for.

Remember that under FOIA, there is a general social need for transparency about the policies, decisions and actions of public bodies. This particularly applies to issues of interest to the wider public and where disclosure demonstrates accountability. For example, disclosing the expenses claims of a public official may be necessary in order to increasing accountability and transparency in the spending of public funds.

However any interference in the data protection rights of your employees must be proportionate. It is likely to be easier to demonstrate a need to release personal information about more senior decision makers than about more junior staff. There is also a greater case for arguing personal expenses should be disclosed where the claims system has no oversight and has been open to abuse.[7]

---

[6] Decision notice FS50125350

[7] *Corporate Officer of the House of Commons v Information Commissioner* [2008] EWHC 1084 (Admin), paragraph 43

If you are dealing with a request where the legitimate interest in disclosure is based solely on the requester's private concerns, you need to bear in mind that:

- disclosure under FOIA involves disclosure to the world at large; and
- information released under FOIA is free from any duty of confidence.

Consequently, if you comply with the request, you are, in effect, making an unrestricted disclosure of your employee's personal data to the general public on the strength of an individual requester's private concerns. A disclosure of this nature could constitute a disproportionate and unwarranted level of interference with your employee's rights and freedoms

This being the case, in our view it is unlikely that a disclosure under FOIA based on purely private interests meets the final limb of the three part test. In such cases it is possible that you could satisfy the requester's private interests by a restricted disclosure to the requester outside FOIA, and that therefore a disclosure into the public domain is not necessary. It is also unlikely that a purely private interest equates to a pressing social need.

Types of information

The factors listed above are described in general terms. It is not possible to lay down specific and absolute standards about what you should disclose, and you have to consider the circumstances of the case for each FOIA request.

As a guide, the following sections consider how the factors discussed above apply to some of the main types of information about public authority employees. They discuss some of the key issues about these types of information, but in any particular case you need to consider other aspects of the approach to section 40 outlined in our guidance on personal information.

Salaries and bonuses

In recent years public authorities have published an increasing amount of information on salaries of public sector officials.

Government departments and other public bodies now routinely publish the names, job titles and salaries of senior civil servants on www.data.gov.uk, as part of the government's policy on open data and transparency. Salaries are given in bands of £5,000 (eg £120,000 to £124,999). For more junior posts the job title and pay scales are shown.

It is well-established practice that local authorities, fire and police authorities and certain other public bodies in England publish salary-related information in their annual accounts. For example, for each employee who earned over £50,000 in the previous year, they publish actual salaries, allowances, bonuses, compensation and employer's pension contributions. This also includes the names of those staff who earned over £150,000.

You should include details in your publication scheme of the information you routinely make available. Remember that information on salaries which is already published and accessible to requesters is likely to be exempt from disclosure under FOIA section 21 (information accessible to the applicant by other means).

However when considering the legitimate interests test for salary information which is not routinely published, you should consider how much significant information you are disclosing about an individual's personal financial circumstances. It is clear that more detailed information or exact salaries are more intrusive than giving a salary band or the pay scale for a post.

For example, if salaries are individually negotiated or contain a significant element of performance related pay, disclosure may give significant information about that individual, and could have a detrimental effect on them.

Seniority is also a factor. If you make a cut-off point in the salary scale (derived, for example, from statute or a code of practice) then you should create a reasonable expectation about who you routinely publish detailed salary information about.

Of course, there is a legitimate public interest in knowing how public money is apportioned across an organisation, which includes salaries at lower levels. Therefore, for more junior staff, you might

disclose the advertised salary range for these posts in bands of £5,000.

You may be able to break down bonus payments into bands in the same way for disclosure. However, this is not a definitive rule and what is appropriate depends on the circumstances. You should take a proportionate approach, balancing the public interest in disclosure and the privacy rights of the employee, and taking account of the sector in which you operate.[8]

Exceptional circumstances are needed to justify the disclosure of exact salaries when you don't routinely published them. In such cases there may be additional public interest factors that outweigh any detriment to the employees concerned. These exceptional circumstances could include situations where:

- there are current controversies or credible allegations;
- there is a lack of safeguards against corruption;
- normal procedures have not been followed;
- the individual in question is paid significantly more than the usual salary for their post; or
- the individual or individuals concerned have significant control over setting their own or others' salaries.

Remember you should only disclose enough information to meet the legitimate interests identified. If the information goes beyond what is necessary to meet the legitimate public interest, then there is no basis for processing and disclosure is in breach of UK GDPR principle (a). In these circumstances, the information is exempt under FOIA section 40(2).

Termination of employment

These requests relate to issues such as severance payments, compromise agreements and circumstances in which an employee leaves your organisation. As with other requests for employee information, your consideration of the legitimate interests balancing test usually involves considering the employee's reasonable expectations.[9]

In assessing these expectations, you have to take account of statutory or other requirements to publish information and also the increasing public expectation of transparency regarding the expenditure of public money and the performance of public

[8] Decision notice FS50363389
[9] Decision notice FS50349391

authorities. This is especially the case if there is any evidence of mismanagement by senior staff in a public authority.

The general issue of lawfulness under principle (a) is also relevant to the disclosure of compromise agreements.

A compromise agreement is likely to contain a confidentiality clause and our view is that disclosure is unlawful if it was in breach of an enforceable contractual term. However, you cannot simply contract out of your obligations under FOIA. Whether a confidentiality clause applies in any particular case depends on whether the specific information is truly confidential.

Lists, directories and organisation charts

You may receive a request for the names of employees, for example the names of all employees above a certain level or for a directory or organisation chart listing all your staff. The requester might also ask for job titles or direct contact details.

Most authorities publish the details of their most senior employees, such as their Chief Executive and Directors of departments, on their website and in other material. The section 40 exemption therefore does not arise in respect of this information.

Organisational structure charts are also routinely made available. For example, government departments publish organograms or structure charts on www.data.gov.uk showing the job titles and reporting lines for all their posts.

This does not mean that there is a requirement to publish the names of all the post holders; usually only the names of senior managers are published. If a request is received for names below this level, the issue in terms of section 40 is whether it is reasonable to disclose these in the context of the specific request. It is not possible to establish a single cut-off point for all authorities, below which names will never be disclosed.

The more senior an employee is and the more responsibility they have for decision making and expenditure of public money, the greater their expectation should be that you disclose their name.[10] However, seniority within the organisational structure is not the sole determining factor. Employees who represent their authority to the outside world should also expect that their authority will disclose their names.[11]

[10] Decision notice FS50146907
[11] Decision notice FS50276863

Job descriptions

When the requested information relates only to a post, without reference to an identifiable individual who holds that post, it does not constitute personal data. Therefore, a record that a post with certain responsibilities exists in an authority is not in itself personal data. However, a record that an individual holds a certain post, and so has certain responsibilities, is personal data about them.

The job description for a post does not in itself constitute personal data about anyone who may happen to hold that post. However, if the post holder is identifiable from that job description, or from the job description and other available data, then this is personal data. For example, if the name and job title of the post holder are shown on the authority's website, then the post itself becomes the personal data of that individual.

The fact that a person holds a particular post is information about their working life, rather than their private life, and as discussed above, there should be a greater expectation that you will disclose this. However, there may be circumstances in which this may have an adverse effect on them as an individual and may affect their private life. For example, if it were made public that a person has a particular job, or works at a particular location. You need to consider this as part of the legitimate interest test, weighing up the legitimate public interest in transparency against the interference in their rights as individuals.

Names in documents

It is often the case that information requested under FOIA includes the names of employees. For example the author of a document, the senders or recipients of internal emails or the attendees at a meeting. You should follow the general approach outlined above and in the personal information guidance to decide whether it is reasonable to release this information.

If the nature of the information is such that disclosing the name of an employee causes them harm or distress, then you may well judge that you should not disclose the information, for example if it exposed them to threats or reprisals.

In assessing whether employees can have a reasonable expectation that their names are not disclosed, key factors include their level of seniority and responsibility and whether they have a public facing role where they represent the authority to the outside world.

A junior employee whose name appears on an email simply because they are organising a meeting or distributing a document in an administrative capacity has a reasonable expectation that you do not disclose their name.

It is also necessary for you to consider what constitutes the legitimate interest in disclosure. If a request concerns the reasons for a particular decision or the development of a policy, there may be a legitimate interest in full transparency, including the names of those officials who contributed to the decision or the policy.

The decision as to whether it is reasonable for you to release the names therefore depends on a number of factors and you must base it on the circumstances of the request.[12]

Registers of interests

Many public authorities maintain a register of interests in which senior staff are required to record certain information. For example, business interests, shareholdings, property ownership and other outside interests, such as membership of clubs and societies. These are interests that could potentially give rise to a conflict of interests with their position in the organisation.

You may need to record this information in order to monitor any potential conflict of interest, and the scope of the register could include officers below the most senior level who nevertheless make decisions affecting the public or involving the expenditure of public money.

If this information is requested under FOIA, the public clearly have a legitimate interest in knowing that any potential conflicts are monitored and that the decisions and actions of officials are not influenced by their private interests. There is a legitimate interest in transparency in order to foster trust in public authorities.

At the same time, by its nature, such information is primarily about the private lives of these officials. You must therefore consider what information it is reasonable to release. Relevant factors include the seniority of the employees concerned and the extent to which disclosure impacts on their private lives.[13]

[12] First-tier Tribunal, paragraph 25 EA/2009/0035
[13] First-tier Tribunal, paragraph 29 EA/2011/0131 & 0137

Disciplinary files

In some cases it may be appropriate for you to neither confirm nor deny that you hold information on an employee.

FOIA section 40(5A) and (5B)(a) and EIR regulation 13(5A)(a) and 13(5B)(a) state that the duty to confirm or deny whether you hold information does not arise if giving the confirmation or denial itself contravenes the data protection principles.

This can arise, for example, if you receive a request for information about disciplinary investigations. You must consider whether it is unfair to an employee for you to confirm (or deny) that they have been disciplined or are the subject of an investigation.[14]

Please also see our specific guidance on Access to information in complaints files.

Representatives of other organisations

As well as receiving requests about your own staff, you may receive requests that involve disclosing the names of employees or representatives of other organisations. For example, people from outside organisations who attended a meeting with your authority.

The fact that someone has attended a meeting, albeit as a representative of another organisation, is personal data about them. Therefore, as with other requests for third party personal data, the question is whether disclosure is exempt under section 40(2) because it contravenes the data protection principles.[15]

The more senior the representative of the other organisation, the more likely it is that it is reasonable to release their names.

Also, if someone normally acts a spokesperson for the other organisation, disclosure of their name is more likely to be reasonable. This is particularly the case when the other organisation is lobbying the public authority in order to influence it. In such cases there should be a general expectation that the names are released.[16]

[14] Decision notice FS50391625
[15] First-tier Tribunal, paragraph 19 EA/2007/0072
[16] First-tier Tribunal, paragraph 70 EA/2008/0065

Good practice

You should list in your publication scheme the information about employees that you routinely make available, such as organisation charts and salaries of senior staff or salary ranges. This includes information that you are required to publish by law or that you publish to meet the requirement for greater transparency in the public sector. Read our guidance on publication schemes for more information.

As a data protection controller, you have a duty to ensure that employee data is adequately protected, but you also have a duty to respond to requests under FOIA. You should not create unreasonable expectations amongst your employees about what data is withheld.

You should have a general policy on releasing employee information in response to FOI requests. Such a policy should be reasonably constructed, avoiding, for example, a simple cut-off point based solely on grade or seniority. It should also take account of the requirement for greater transparency.

While you must consider each request on its own terms, having a general policy helps employees to form a reasonable expectation of what information may be released about them. It also assists potential requesters to see what information you are likely to release. As an example, the ICO's policy on disclosure of employee information is published on our website. This reflects our own situation as a public authority and the criteria in our policy may not necessarily apply to other authorities.

It is not possible to envisage every type of request in a general policy. In novel or controversial cases, you should be prepared to consult with employees and take account of their views, while recognising that their wishes do not ultimately determine whether you should release the information. It is up to you to decide whether to release information, following the criteria and the approach outlined in our guidance.

More information

This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. We will regularly review the guidance and keep it in line with

new decisions of the Information Commissioner, tribunals and courts.

It is a guide to our general recommended approach, although we will always assess individual cases on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information or data protection, please contact us or see our website www.ico.org.uk.