**INFORMATION SHARING AGREEMENT BETWEEN**

**THE MAYOR AND BURGESSES OF THE LONDON BOROUGH OF HAMMERSMITH AND FULHAM (“H&F”)**

**and**

**TPAS LIMITED**

**for**

**Independent Tenants’ & Leaseholders’ Advisory Services**

**01/05/2015**

**Review date 31/01/2016**

**Table of contents**

[1. Introduction 2](#_Toc406683903)

[2. Objective of the Agreement 3](#_Toc406683904)

[3. Legal basis for sharing personal information 3](#_Toc406683905)

[4. Participants to the Agreement 3](#_Toc406683906)

[5. Purpose(s) for which information is to be shared 4](#_Toc406683907)

[6. Types of information to be shared 4](#_Toc406683908)

[7. Data handling requirements 5](#_Toc406683909)

[8. Data protection legislation and guidance 7](#_Toc406683910)

[9. Practical application of the Data Protection Act 1998 7](#_Toc406683911)

[9.1 The 8 principles of the Data Protection Act 1998 7](#_Toc406683912)

[9.2 Notification under the Data Protection Act 1998 7](#_Toc406683913)

[9.3 Notifying data subjects or seeking consent for the information sharing 8](#_Toc406683914)

[9.4 Disclosure to third parties 8](#_Toc406683915)

[9.5 Related legislation 9](#_Toc406683916)

[10. Accountability under this agreement: roles and responsibilities 10](#_Toc406683917)

[10.1 Authorised officer 10](#_Toc406683918)

[10.2 Designated senior officer 10](#_Toc406683919)

[10.3 Staff obligations 10](#_Toc406683920)

[10.4 Review of the Agreement 10](#_Toc406683921)

[10.5 Withdrawal from the Agreement 10](#_Toc406683922)

[Appendix A: The Agreement contract 12](#_Toc406683923)

[Appendix B: The Data Protection Principles 13](#_Toc406683924)

[Appendix C: Conditions Relevant for Purposes of the First Principle: Processing of any Personal Data 16](#_Toc406683925)

[Appendix D: Conditions Relevant For Purposes of the First Principle: Processing of Sensitive Personal Data 17](#_Toc406683926)

[Appendix E: Designated Officers 20](#_Toc406683927)

# Introduction

The legal basis for sharing personal information is enshrined in the Data Protection Act 1998 (the Act). The Act sets out 8 Principles that provide the parameters for how personal information should be collected, maintained, shared and disposed. All information sharing arrangements must be able to demonstrate compliance with these Principles [Appendix B] where personal information is being processed. Other legislation or regulation governing information sharing, include the Crime & Disorder Act, Section 75 National Health Service Act 2006, Caldicott Principles, Local Government Act 1972.

This information sharing agreement (the Agreement) is an operational document flowing from the contract between H&F and the appointed adviser that defines the nature of the sharing, the roles and responsibilities of the Data Controllers and Processors and provides mutual consent to share between the Data Controllers and Processors. The Agreement provides the details necessary to ensure the actual sharing of personal information complies with the Act. For example, what information will be shared, why, how and with whom.

The Agreement applies to situations where the sharing of personal information is essential to the delivery of the Strategic Housing Stock Options Appraisal and Residents’ Commission for the London Borough of Hammersmith and Fulham (H&F), their service delivery partners, and the third party contractor fulfilling the role of Independent Tenant Adviser and named in this document.

# Objective of the Agreement

The outcome of the Strategic Housing Stock Options Appraisal and Residents’ Commission will direct the future model for the provision of a significant proportion of affordable housing within H&F. To enable transparency and effectiveness it will be necessary for a wide range of expertise, including tenant expertise to work together efficiently, meeting the timetable for achieving implementation of the preferred model. The sharing of information will be a crucial element of this efficiency, transparency and effectiveness.

The Independent Tenant Adviser will provide independent advice and support to tenants and leaseholders throughout the stock options appraisal. Should stock transfer or another option resulting in the creation of a new separate organisation(s) be recommended the adviser will offer the same expertise to support the ensuing pre ballot, consultation and post ballot phases of the transfer of its housing stock. In order to be effective in this role the adviser will need to have sight of H&F data, including tenant data.

# Legal basis for sharing personal information

On 1st December 2014, the Council’s Cabinet authorised a Strategic Housing Stock Options Appraisal (SHSOA) to consider the options for empowering residents to take local control over their homes and for maximising investment in existing and new council homes. The guiding statute applicable to this process is: “The Housing Act 1985: Schedule 3A – consultation before disposal to private sector landlord.” The outcome of this appraisal together with a recommend preferred option is expected to report back to Cabinet in September 2015 which practically means having the options appraisal concluded by June 2015. This agreement is in support of the issued contract for the Independent Tenant Adviser supporting these activities.

The Independent Tenant Adviser Contract was issued to TPAS Ltd on May 2015.

Therefore processing is necessary for the purposes of legitimate interests pursued by the data controller (H&F) in order to inform the options appraisal process and the communications activities that will support it.

# Participants to the Agreement

The services and contractors participating (the Parties) in this Agreement are as per the signatories in Appendix A include:.

1. **London Borough of Hammersmith and Fulham**, Information Commissioner Registration Number: Z5124889, Date of Renewal: 18 December 2012 (data controller)
2. **TPAS Limited**, Information Commissioner Registration Number: Z9333856, Date of Renewal: 10 01 2016 (data processor).

While sub-contracting is not currently envisaged or agreed, in the event of any sub-contracting elements of the service in the future, any such sub-contractor has to comply with a version of this ISA too.

Data control will rest with H&F, with all parties adhering to the data protection measures and protocols of H&F, incorporating these into their own measures and protocols for all information under this agreement.

# Purpose(s) for which information is to be shared

As stated in the above objective, information will be shared to enable effective cross communication between all the parties: H&F, appointed advisers, nominated contractors and residents. Consent to the sharing of information is part of the project specification, contract specification, and participation agreement respectively.

# Types of information to be shared

Information shared in both electronic and written formats, in data sets, individual elements and structured detail will be:

* Individual contact details of all project parties to enable contact.
* Company details of contractors with tenant contact to enable confidence and transparency.
* Council stock profile and economic data with tenants and contractors to enable quantitative and fiscal understanding of options.
* Tenant details, to enable contact, and to enable diversity and demographic assessment evaluation of communication.
* Diversity and demographic summary data at specific community sub-level groupings to aid targeting within communication strategy and conduct.
* Diversity and demographic individual data to enable diversity and demographic assessment evaluation of opinion monitoring and trends.

The Personal Data aboveare and will remain the responsibility of H&F at all times.

# Data handling requirements

The Responsible Persons for each Party is as follows: -

* H&F – Geoff Wharton, Interim Director of Housing Services
* TPAS Ltd, Emma-Jane Flynn, Consultancy Manager South

For the duration of the agreement, the ITA Adviser will not receive IT access to H&F Systems.

The Programme Board will ensure that a quarterly standing agenda item will be included on the ITA Adviser’s review meetings to review and monitor the ITA Adviser’s compliance with the Information Sharing Agreement.

Information will be shared for the duration of the project, which is to last a maximum of three years. All shared data will be subject to the Data Controller’s (ie H&F) data protection and retention policies, with the exception of shared tenant data which will be destroyed by all parties other than H&F at the conclusion of the project. Tenants will be subject to H&F policy for those involved tenants, otherwise the information received by tenants on a wider basis will already comply with data protection guidance and regulation.

In particular, but not exclusively, the following sections of the H&F Information Security Policy will apply (with advisory links shown for reference):

*07 Reporting information security incidents*

*An information security incident is when council or personal information or devices holding such information is lost, stolen or inappropriately disclosed or shared with a 3rd party. It includes a potential breach of the Data Protection Act 1998. H&F have established procedures to ensure that it reacts appropriately and swiftly to any actual or suspected incidents relating to information systems and information held by the council.*

* *Report any incidents or suspected incidents immediately, e.g. if you lose your Blackberry or have your laptop stolen.*
* *Instructions on how to report can be found on the IT Matters <*[*http://theintranet/IT\_Matters/Service\_Desk/80612\_Security\_Incidents.asp*](http://theintranet/IT_Matters/Service_Desk/80612_Security_Incidents.asp)*> website.*
* *Detailed guidance on handling information security incidents and an incident toolkit can be downloaded from the Information Security Pages <*[*http://theintranet/IT\_Matters/Service\_Desk/80612\_Security\_Incidents.asp*](http://theintranet/IT_Matters/Service_Desk/80612_Security_Incidents.asp)*> on H&F's intranet*
* *Incidents involving health or adult social care information must follow additional reporting process to notify the Department of Health, ICO and other regulators. Further guidance is available from the ICO's webpages on Reporting Security Breaches*

 *<*[*http://ico.org.uk/for\_organisations/data\_protection/lose*](http://ico.org.uk/for_organisations/data_protection/lose)*> .*

Link to Information Security Policy:

<<http://theintranet/Council_Business/Business_Technology/Information_Security/171123_Information_Security_Policy_00_Introduction.asp>

The Independent Tenant Adviser shall employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure and comply with the Council’s Information Security Policy. The adviser will take all the steps outlined as mitigation in the Privacy Impact Assessment, such as, but not exclusively: all sensitive personal data to be encrypted when sent by email outside of the H&F network using Egress Switch; all papers to be transferred and stored securely; all information to be securely destroyed using H&F’s confidential waste service. The organisational, operational and technological processes and procedures adopted are required to comply with the requirements of ISO/IEC 27002-2:2005 (ISO/IEC 17799:2005) as appropriate to the services being provided to the Council. H&F will use ISO/IEC 27002-2:2005 as a basis for auditing compliance in relation to this obligation.

The Independent Tenant Adviser will not keep the personal data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use of the device or laptop is necessary for the provision of the services under this agreement. Where this is necessary, the Independent Tenant Adviser will keep an audit trail of which laptops/drives/devices the personal data are held on.

The data will be held by the Independent Tenant Adviser as per agreed and established retention and disposal periods for this data. Reference is to be made to the document ‘*A Retention Schedule for Information Received or Created by Local Authorities’*, [file name: Batchelor's LA Retention Schedule-v2 3 20141230\_tcm19-192823].

The Independent Tenant Adviser shall ensure that only such of its employees who may be required by it to assist it in meeting its obligations under the Agreement shall have access to the Personal Data.

The Independent Tenant Adviser shall ensure that all employees used by it to provide the services as defined in the Agreement have undergone training in the law of data protection, their duty of confidentiality under contract, and in the care and handling of Personal Data and have signed the Communication Adviser’s respective Information Security policy commitment.

The Independent Tenant Adviser agrees to assist H&F promptly with all subject information requests which may be received from the data subjects of the Personal Data, in line with the deadlines specified by H&F in order to remain with the DPA’s statutory timelines.

The Independent Tenant Adviser shall not disclose the Personal Data to a third party in any circumstances. The third party can seek access via H&F’s access to information processes under FOIA, EIR and the DPA.

# Data protection legislation and guidance

The Act governs the protection and use of personal information identifying living individuals. It gives individuals rights in relation to the handling of their personal information by organisations. Organisations must handle this information in accordance with all the standards in the Act known as the Data Protection Principles. These are outlined in Appendix B.

This Agreement does not seek to supersede the principles and regulatory framework that is the Act, any subordinate or related legislation, orders or judgements. In the event of conflict between any part of this Agreement and any legislative or policy requirement in place, the latter will take precedence and that part of the Agreement deemed to be in conflict will be considered suspended until the Agreement is reviewed and, if necessary, revised.

# Practical application of the Data Protection Act 1998

## The 8 principles of the Data Protection Act 1998

Please ensure that all the principles of the Act are complied with. Full details are available in Appendix B.

This Agreement does assist your compliance with these principles but it may be advisable to complete a privacy impact assessment for the project or new service you are about to embark upon.

## Notification under the Data Protection Act 1998

It is the responsibility of each participating organisation to ensure that the handling of personal data under this agreement is included in their Notification to the Office of the Information Commissioner as required under the DPA.

## Notifying data subjects or seeking consent for the information sharing

Individuals **must** be made aware that their information will be shared for the purpose of this Agreement. It is a requirement of Principle 1 of the DPA that where an organisation obtains personal data, they must ensure that the individual is aware not only of the **reason** for which such information is being collected but also aware of with **whom** it may be shared. This need only be done once; it is neither practicable nor necessary to seek an individual's specific consent each time that information is passed on for a particular purpose that has been defined in this Agreement. Each signatory to this Agreement will need to demonstrate that this requirement has been fulfilled.

In some cases, where **sensitive personal data** is to be shared, **participating organisations/departments will need to obtain explicit consent** for the sharing unless they can satisfy another condition under Schedule 3 of the DPA (see Appendix D).

In either case where consent has been sought, it is important to note that individuals are entitled to withdraw their consent at any time. Where an individual contacts the participating organisation/department to withdraw their consent - subject to any exemptions that may apply - the participating organisation/department **must** advise all other parties to this Agreement and the individual’s data must not be handled for the purpose(s) of this data sharing arrangement.

## Disclosure to third parties

Personal information should only be disclosed for the purpose identified in section 4 (Purpose for which information is to be shared) and in accordance with what the individual has been told. There are exceptions if the information is required for the following purposes:

* the disclosure is necessary for the prevention 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 (s.29)
* the disclosure consists of information which is required by law to be made publicly available (s.34)
* the disclosure is required by law or by order of the court (s.35(1))
* the disclosure is made in connection with legal proceedings (s.35(2))

Outside of section 35(1) none of the above caveats are mandatory, which means that disclosures will have to be considered on a case-by-case basis. Generally, disclosure should be proportional and must consider the Rights of third parties whose personal data may also be present. Each signatory should ensure that they consult with their Data Protection officers prior to disclosure, as well as documenting and informing other signatories of the disclosure. Where the information has been provided by a medical practitioner, the owner of the data will be responsible for ensuring that their consent has been obtained to the disclosure.

## Related legislation

**The Common Law Duty of Confidentiality**

The Common law duty of confidentiality may apply to a large amount of information obtained by an organisation. As a general principle the duty arises where a person receives information in situations where it is known or can be taken to be known that the information is to be treated as confidential.

Whenever information is obtained in circumstances where a duty of confidence is to be inferred, there is a legal duty to respect the confidentiality of information provided and not to disclose it to third parties without consent, unless an overriding public interest requires it. Under common law there is a duty to act reasonably and in a manner that is proportionate to the aim. Information obtained in confidence should not be disclosed to a greater extent than is necessary in the interests of the individual.

Generally, it will be possible to satisfy legal obligations under the common law duty of confidentiality if the personal information is handled in a manner that complies with the obligations as set out in the Data Protection Act.

**The Human Rights Act 1998**

The Human Rights Act prohibits interference by a public authority with the private and family life of individuals, their homes and correspondence, save where that interference is lawful and necessary in a democratic society, public safety, the protection of rights and freedoms of others, the prevention of disorder or crime and the protection of health and morals.

Interference with an individual’s privacy must not be disproportionate even where it is in pursuit of such aims as allowed by the Human Rights Act. In addition, the handling of an individual’s personal information should only be limited to pursue the objectives for which the information was collected.

**Freedom of Information Act 2000/Protection of Freedoms Act 2012 (part 6: freedom of information and data protection)**

The Freedom of Information Act (FOIA) provides for a general right of access to official information held by public authorities (subject to the exemptions contained in the FOIA), and as each of the partners is a public authority there is a statutory duty to handle requests for information in accordance with the framework of the FOIA. Where the data sharing Protocol involves another public authority(s), it will be the duty of the recipient public authority to handle the request in accordance with the legislation. Each signatory should make proper arrangements to enable information to be shared and disclosed in relation to non-personal data.

The Protection of Freedoms Act (part 6) extends the FOIA in the following ways for the UK:

* section 102: the release and publication of datasets held by public authorities
* section 103: definition of “publicly owned company”

# Accountability under this agreement: roles and responsibilities

## Authorised officer

This Agreement must be signed by a senior authorised officer for each participating organisation/department (see Appendix A).

## Designated senior officer

Each Authorised Officer should nominate at least one senior officer within each participating organisation/department responsible for agreeing amendments to the Agreement, monitoring and reviewing its operation and ensuring compliance. Designated seniors officers and contact details are listed at Appendix E. For the purposes of this contract the nominated contract manager / consultant employed on the project will be the designated officer for their respective organisation by exception.

## Staff obligations

It is the responsibility of each participating organisation/department to ensure that staff with authorised access to the data covered by this Agreement are aware of their obligations under the DPA to safeguard that information. Staff should be aware that breach of the controls contained within this Agreement could be a matter for disciplinary action and may provide grounds for a complaint under the DPA against them which may result in criminal or civil action against them.

## Review of the Agreement

All elements of this Agreement will be reviewed every 12 months.

## Withdrawal from the Agreement

If any party wishes to withdraw from this Agreement, they must give six weeks written notice of this intent. Letters will be addressed to the signatories of the Agreement at the addresses shown in Appendix A. Individuals whose data has been hitherto shared must be informed where a participating organisation/department has withdrawn from the data sharing arrangement.

Any Party who withdraws **must** ensure that all data is reviewed and deleted. Withdrawal is automatic with termination of the contract through which a signatory is part of this agreement, however the signatory is obliged to conform absolutely with the review and deletion requirement as of the date of their termination becoming in force.

#

# Appendix A: The Agreement contract

**Agreement for sharing personal information between the London Borough of Hammersmith and Fulham and the Independent Tenant Adviser**

**AGREEMENT**

For and on behalf of **LONDON BOROUGH OF HAMMERSMITH AND FULHAM**

We, the undersigned, do hereby agree to implement the full range of measures outlined in this Agreement.

For and on behalf of … London Borough of Hammersmith and Fulham…

Signature:

Name:

Position:

Address:

Date:

For and on behalf of **TPAS Limited**

Signature:

Name:

Position:

Address:

Date:

# Appendix B: The Data Protection Principles

**Principle 1**

“Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.”

Participating organisations/departments should ensure that the sharing of personal data under this agreement is lawful and does not contravene any lawful power to which they may be subject. Where the organisation's functions are determined by statute (eg. local authorities or other statutory bodies) then it must be ensured that they are not acting *ultra vires* in participating in this data sharing arrangement. In addition, participating organisations/departments must ensure that the sharing of data meets at least one of the conditions of processing in Schedule 2 of the Act (see Appendix C for list).

**Principle 2**

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.”

Principle 2 of the Act states that "personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or these purposes".

The purpose for sharing data under this agreement l should be compatible with the purpose for which the personal data was originally obtained by the participating organisation/department. Where the data is being shared for a non-compatible purpose, each owner of the data must seek the permission from the data subject for the secondary use of their personal data. This should be done prior to any sharing for secondary use, or as reasonably practicable.

**Principle 3**

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.”

In line with Principle 3 of the Act, it is essential that the data collected by the organisation/department and that which is shared with other parties is the minimum identifiable information necessary for the purpose of this data sharing arrangement.

**Principle 4**

“Personal data shall be accurate and, where necessary, kept up to date.”

It is the responsibility of each participating organisation/department to ensure and maintain the accuracy of personal information they share with other organisations under this Agreement. Where an organisation/department becomes aware that information they have provided may be inaccurate, they **must** take steps to inform all participating organisations/departments of the updated data.

**Principle 5**

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.”

Unless a statutory period applies, data which is kept for the purpose of this data sharing arrangement should only be kept for as long as necessary in line with agreed policies. Participating organisations/departments should agree and document a standard period for which the information will be retained, a procedure for how the data will be reviewed and agree on secure disposal methods. Where personal data is being processed this is **Mandatory**.

**Principle 6**

“Personal data shall be processed in accordance with the rights of data subjects under this Act.”

Under the Act, individuals have rights to have access to personal information about them held by any organisation. Subject access requests must be fulfilled within 40 calendar days. Each participating organisation/department has responsibility for ensuring that individuals are provided with access to personal information held about them in accordance with the requirements of the Act. Please refer to the H&F Information Management Portal for more advice.

**Principle 7**

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

Each participating organisation/department must take all reasonable care and employ appropriate physical, technical and organisational safeguards to the personal data under this data sharing arrangement. Participating organisations/departments must agree on the standards required for protecting the data, for example, the storage safeguards for information in hardcopy and electronic format, security of data in transmission, security standards for access to the data. Higher safeguards will be required where the personal data is of a sensitive nature.

Staff should only have access to personal data in order to perform their duties in connection with one or more of the purposes defined in section 3 (Purpose for which information is to be shared). Technical and physical safeguards should be in place to restrict access to the information only to authorised staff for example, password control. These should be in line with agreed policies and procedures

**Principle 8**

“Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”

# Appendix C: Conditions Relevant for Purposes of the First Principle: Processing of any Personal Data

1. The data subject has given his consent to the processing.
2. The processing is necessary-
	1. for the performance of a contract to which the data subject is a party, or
	2. for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary-
	1. for the administration of justice,
	2. for the exercise of any functions conferred on any person by or under any enactment,
	3. for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
	4. for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

# Appendix D: Conditions Relevant For Purposes of the First Principle: Processing of Sensitive Personal Data

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary-

(a) in order to protect the vital interests of the data subject or another person, in a case where-

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing-

(a) is carried out in the course of its legitimate activities by any body or association which-

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing-

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by-

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing-

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

# Appendix E: Designated Officers

|  |  |  |  |
| --- | --- | --- | --- |
| **PARTICIPATING ORGANISATION/DEPARTMENT** | **NAME OF DESIGNATED OFFICER** | **POSITION AND RESPONSIBILITY** | **CONTACT DETAILS** |
| London Borough of Hammersmith & Fulham | Mike England | Director of Housing Options | Mike.England@lbhf.gov.uk |
| TPAS Limited | Emma-Jane Flynn | Consultancy Manager | emma-jane.flynn@tpas.org.uk |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |