APPENDIX 4

HILLINGDON
LONDON

Lawful Basis for Processing of Personal Data Policy

May 2018

1. Introduction

1.1 The Council must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others - which basis to use will depend on the Council's purpose and relationship with a particular individual.

1.2 The Council must establish a lawful basis before it begins processing personal data and it is very important that it is **documented and recorded.**

1.3 The requirement to have a lawful basis in order to process personal data is not new. However, the GDPR places more emphasis on bodies such as the Council being accountable for, and transparent about, its lawful basis for processing. **This Policy identifies and explains the important changes which GDPR has introduced.**

1.4 The lawful bases for processing are set out in Article 6 of the GDPR. They are:

1.4.1 the individual has given their consent to the processing of their personal data for one or more specific purposes;
1.4.2 processing is necessary for the performance of a contract to which the Council and the individual is subject to or the Council to take steps at the request of the individual prior to entering into a contract;
1.4.3 processing is necessary for compliance with a legal obligation to which the Council is subject;
1.4.4 processing is necessary in order to protect the vital interests of the individual or of another natural person;
1.4.5 processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council;
1.4.6 processing is necessary for the purposes of the legitimate interests pursued by the Council or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal data, in particular where the data subject is a child.

1.5 If the Council is processing sensitive personal data, it will need to identify both a lawful basis for general processing and also an additional condition for processing this type of data.

1.6 If the Council is processing criminal conviction data or data about offences, it needs to identify both a lawful basis for general processing and also an additional condition for processing this type of data.

2. Consent of the individual

2.1 The GDPR sets a high standard for consent and stipulates that an indication of consent must be unambiguous and involve a clear affirmative action [an opt-in]. Consent can no longer be inferred. **The Council must keep clear written records to demonstrate consent.**

2.2 Explicit consent must be expressly confirmed in words, rather than by any other positive action. There is no time limit set for consent. How long it will last will depend on the context. The Council should review and refresh consent as appropriate.

2.3 **The GDPR gives a specific right to withdraw consent. The Council needs to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.** The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

2.4 The Council is required to make its consent request prominent, concise, separate from other terms and conditions [contained in a written declaration], and easy to understand. It should include:

2.4.1 the name of the Council;
2.4.2 the name of any third party controllers who will rely on the consent;
2.4.3 why the Council wants the data;
2.4.4 what the Council will do with the data; and
2.4.5 that individuals can withdraw consent at any time.

2.5 The Council must ask people to actively opt in. It should not use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, the Council should give separate [granular] options to consent for different purposes and different types of processing.

3. Performance of a contract

3.1 The Council has a lawful basis for processing if:

3.1.1 it has a contract with the individual and it needs to process their personal data in order to comply with its obligations under the contract.
3.1. 2 it has not yet got a contract with the individual, but they have asked the Council to do something as a first step [for example, provide a quote] and the Council needs to process their personal data to do what they ask.

3.2 No significant changes have been introduced by the GDPR.

4. Legal obligation on the Council

4.1 The Council can rely on this lawful basis if it needs to process personal data for the purpose of complying with a common law or statutory obligation. This basis does not apply to contractual obligations.

4.2 The Council should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out its obligation.

4.3 No significant changes have been introduced by the GDPR.

5. Vital interests of an individual

5.1 The Council is likely to rely on vital interests as its lawful basis in circumstances where it needs to process the personal data in order to protect someone's life,

5.2 The Council is unable to rely upon vital interests for health data or other sensitive data if the individual is capable of giving consent, even if they refuse their consent.

5.3 This basis remains substantially unaltered although one key difference under the GDPR is that anyone's vital interests can now provide a basis for processing, not just those of the individual themself.

6. Public task

6.1 The Council can rely on this lawful basis if it needs to process personal data:

6.1.1 'in the exercise of official authority'. This covers public functions and powers that are set out in law [such as a public body's tasks, functions, duties or powers]; or
6.1.2 to perform a specific task in the public interest that is set out in law [statutory and common law].

6.2 The Council does not need to identify a specific statutory power to process personal data, but its underlying task, function or power must have a clear basis in law.

6.3 **The processing must be necessary.** This means that the processing must be a targeted and proportionate way of achieving its purpose. If the Council could reasonably perform its tasks or exercise its powers in a less intrusive way, then this lawful basis does not apply.

6.4 **The Council should as a matter of good practice document its decision to rely on this basis to help demonstrate compliance.** The Council should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

6.5 The Data Protection Act 2018 states that the public task basis will cover processing necessary for:

6.5.1 the administration of justice;
6.5.2 parliamentary functions;

6.5.3 statutory functions; or
6.5.4 governmental functions.

6.6 However, the above is not intended to be an exhaustive list. If the Council has other official non-statutory functions or public interest tasks, it can still rely on the public task basis as long as the underlying legal basis for that function or task is clear and reasonable.

7. Legitimate interests pursued by the Council

7.1 Legitimate interests is considered to be the most flexible basis for lawful processing. The Council can rely upon this basis if it is processing personal data for a legitimate reason other than performing its tasks as a public authority.

7.2 There are three specific elements to the legitimate interests basis. The Council needs to:

7.2.1 identify a legitimate interest **(Purpose test);**
7.2 2 show that the processing is necessary to achieve it **(Necessity test);**
7.2.3 balance it against the individual's interests rights and freedoms **(Balancing test).**

7.3 The legitimate interests can be the Council's own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

7.4 **The processing must be necessary.** This means that the processing must be a targeted and proportionate way of achieving its purpose. If the Council can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

7.5 The Council must balance its interests against the individual's. If they would not reasonably expect the processing, or it would cause unjustified harm, their interests are likely to override the Council's legitimate interests.

7.6 **The Council should as a matter of good practice keep a record of its legitimate interests assessment to help it to demonstrate compliance.**

7.7 The GDPR specifically mentions use of client or employee data, marketing fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that the Council will have a legitimate interest in disclosing information about possible criminal acts or security threats to the relevant authorities.

7.8 **The Council can consider legitimate interests for processing children's data, but it must take extra care to make sure that their interests are protected.**

8. Sensitive personal data

8.1 Article 9 of the GDPR provides that *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying natural person, concerning health or data concerning a natural person's sex life, or sexual orientation shall be prohibited".* (See exceptions below).

8.2 Sensitive personal data needs extra protection. Therefore, the Council will still have to establish a lawful basis for processing the data but the difference here is that it will also need to satisfy a special condition under Article 9 of the GDPR before it is able to process it. It is important to note that these do not need to be linked.

8.3 The conditions for the processing of sensitive personal data insofar as they relate to the Council are:

8.3.1 the individual has given explicit consent to the processing of the data for one or more specified purposes;
8.3.2 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Council or the individual in the field of employment and social security and social protection law;
8.3.3 processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent;
8.3.4 processing relates to personal data which are manifestly made public by the individual.
8.3.5 processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
8.3.6 processing is necessary for reasons of substantial public interest which shall be proportionate to the aim pursued, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual;
8.3.7 processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care treatment or the management of health or social care systems and services pursuant to contract with a health professional;
8.3.8 processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.
8.3.9 processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

9. Criminal offence data

9.1 To process data about criminal convictions and offences or related security measures [collectively known as criminal offence data], the Council must have both a lawful basis under Article 6 of the GDPR and either legal authority or official authority for the processing under Article 10. The concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions but it is wider than this as it is also linked to related security measures.

9.2 The Council is unable to keep a comprehensive register of criminal convictions unless it does so in an official capacity. The Council must determine its condition for the lawful processing of offence data [or identify its official authority for the processing] before it begins the processing **and it should document this.**

9.3 The Data Protection Act 2018, when enacted, will make some changes both to the conditions relating to the processing of sensitive personal data and also the processing of criminal offence data and this Policy will be amended accordingly once the new Act has received Royal Assent.