|  |
| --- |
| Letterhead_Logo_COLOUR |

|  |  |
| --- | --- |
| 23 May 2018 |  |

**Reference: xxx/GDPR**

Dear Supplier

**General Data Protection Regulation (GDPR) and subsequent Data Protection Bill – Actions now required by suppliers of services to Worcestershire County Council**

**Background**

We are writing to you because Worcestershire County Council has a contract with you.

This may be for services or goods, or may be because you have applied to join a DPS but haven't yet been awarded a specific contract for services. If you believe that you are not the correct recipient of this letter please could you forward it to the person within your organisation who is able to provide the information required.

As you are probably aware new data protection legislation, often referred to as the General Data Protection Regulations or GDPR ('the Regulations') is due to come into force on **25th May 2018.** These Regulations will apply to any public or private organisation processing personal data. It is possible that this will include your organisation.

Accordingly, there are also a number of changes that will affect commercial arrangements, both new and existing, with suppliers. The Regulations specify that any processing of personal data, by a Processor, should be governed by a contract with certain provisions included.

If you process any personal data for or on our behalf, you are a likely to be a Processor under GDPR. GDPR specifies that any processing of personal data, by a Processor, should be governed by a contract with certain provisions included and places new specific legal obligations on processors of personal data. For example you are required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a personal data breach.

**Completion of the Assurance Statement**

So that we are able to ensure that both the Council and your organisation is acting properly there are obligations and actions we must ask you to complete to ensure that we both continue to act and operate legally. Please complete the attached Supplier Assurance Statement which may be found at this link: [Supplier Assurance Statement](https://forms.office.com/Pages/ResponsePage.aspx?id=hxj0rDe900WeZUfN5I3IWqBM442wHplMuxaVrKy6fWZUM0hCRVBVQjVEMklaNk9BV1hVUlVYVjFITi4u) so that we can establish compliance with legal requirements.

In answering these questions:

1. Against each question, please answer and delete where appropriate Yes or No .
2. If you are yet to be compliant in any area, please advise us of your plans.

Please complete the assurance statement within 21 days of the date of this letter. This will enable us to deal with any required variations to contracts that are identified. If we do not hear from you by then we may take non-compliance action.

More information about doing business with the Council under GDPR may be found on the Council's website: <http://www.worcestershire.gov.uk/gdprbusiness> and more general GDPR information on the Information Commissioner's Office (ICO) website: [http://www.ico.org.uk](http://www.ico.org.uk/)

Yours sincerely

**Andrew Spice**

Director of Commercial and Commissioning

**GDPR – Obligations on Controllers and Processors**

Controllers (in this case the Council) may only appoint Processors (in this case your organisation) that provide sufficient guarantees to ensure processing meets the requirements of the GDPR. Processors are required to process personal data in accordance with the Controller's instructions. It is in the interest of both Controller and Processor to make sure obligations and requirements placed upon the Processor are set out as clearly as possible.

We are writing to all our suppliers to ensure that these new regulation are understood and to ensure that where you process personal information on our behalf or on the behalf of our customers, we are both meeting our legal requirements.

The Council needs to establish that our Processors:

1. Will only act on our written instructions unless otherwise required by law
2. Will follow our instructions regarding the deletion or return to WCC of all personal data when the contract ends, (unless the Processor is required to retain the personal data by law)
3. Will employ persons who are contractually committed to confidentiality or are under a statutory obligation of confidentiality
4. Will ensure that appropriate technical and organisational measures are taken to ensure the security of the processing
5. Will only use sub-processors with our prior written permission and only within a binding written contract with the sub-processor
6. Will assist us in providing subject access and allowing data subjects to exercise their rights
7. Will assist us in meeting our GDPR obligations in relation to the security of processing and data protection impact assessments
8. Will report any data breaches affecting personal data processed on our behalf without undue delay and ensure prompt investigation is undertaken
9. Will be able to demonstrate at any point that compliance is being met and will maintain a record of all processing, including subject matter and duration of the processing, the nature and purposes of the processing, types of personal data and the categories of individuals, being carried out on our WCC
10. Will appoint a Data Protection Officer (DPO) where necessary
11. Will submit to audits and inspections, and provide us with whatever information it needs to ensure that you and us are both meeting their GDPR obligations, and tell us immediately if you are asked to do something infringing the GDPR or other data protection law
12. Will limit data transfers to third countries only to countries or organisations where appropriate safeguards have been put in place and in all circumstances only with our prior written agreement

**Definitions**

|  |  |
| --- | --- |
| Controller | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.  In the DPA 1998 this was a 'Data Controller' |
| Data Protection Officer (DPO) | GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority, or if you carry out certain types of processing activities. A DPO is an independent expert on data protection who works to ensure an organisation is adhering to the requirements of GDPR |
| Information Commissioner's Office (ICO) | UK’s independent supervisory authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals |
| Personal Data | Any information relating to an individual (‘data subject’); who can be identified, directly or indirectly, from the information. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual |
| Personal Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed |
| Processing | Any operation or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means.  Examples include: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction. erasure or destruction |
| Processor | A natural or legal person, public authority, agency or other body which processes personal data **on behalf of** the Controller  In the DPA 1998 this was a 'Data Processor' |