**BACKGROUND PAPER FOR AGENDA ITEM FOR APRIL MEETING**

**GDPR - DATA PROTECTION OFFICER**

The General Data Protection Regulations *(‘GDPR’)* require all public authorities to appoint a Data Protection Officer *(‘DPO’)*. The DPO’s minimum tasks are defined as:

* to inform and advise the organisation *[sic – Sutton at Hone & Hawley Parish Council]* and its Members and employees about their obligations to comply with the GDPR and other data protection laws;
* to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities and advise on data protection impact assessments and
* to be the first point of contact for supervisory authorities and for individuals whose data is processed

The GDPR provides that the DPO operates independently and is not to be dismissed or penalised for performing their task. The DPO is required to report to the Chairman of Sutton at Hone & Hawley Parish Council *(‘the Council’)*.

No instruction must be given to the DPO regarding how to deal with a matter, what results should be achieved or whether or not to consult with the Information Commissioners Office (*‘the ICO’)*. As a matter of good practice, reasons for not following the DPO's advice should be documented.

Advice given is that –

1. The appointment of a DPO must be based on personal and professional qualities, with particular attention to expert knowledge of data protection, a good understanding of the way the Council operates is also recommended. The DPO is an integral part of the Council, making him/her ideally placed to ensure compliance, nevertheless, the DPO should be able to perform his/her duties independently, the number of assurances guaranteeing this independence include:

* the DPO will not receive any instructions regarding the performance of his/her duties;
* there should be no conflict of interest between the duties of the DPO and his/her other duties and specifically, the DPO should not determine the purpose or manner of processing personal data;
* the DPO should have the authority to investigate and have immediate access to all personal data and data processing operations and to be provided with information in reply to his/her questions.

1. Importantly, it is the Council and not the DPO personally, which remains responsible for compliance with the GDPR, although appointment of and adherence to the guidance of the DPO may assist in demonstrating compliance with GDPR requirements.
2. Publication of the DPO’s contact details is required by the GDPR. The name of the DPO does not need to be made publicly available but should be notified to the ICO and members of staff. Members of the public need only to be given sufficient information to enable communications to easily reach the DPO (e.g. a dedicated email address published on the Council’s website).

It should be noted that the Clerk has for many years acted as the Council’s DPO to –

* ensure data protection compliance within the Council and assisting it to be accountable in this respect;
* ensure data subjects are informed about their data protection rights;
* advise and recommend on the interpretation or application of the data protection legislation;
* handle queries or complaints on data protection related issues;
* co-operate with the ICO when responding to complaints on data protection related issues;
* draw the Council’s attention to any failure to comply with data protection legislation;

The Clerk also deals with broader information governance duties, including FOI requests, and provides corporate oversight of information (including, but not limited to personal information) across the Council.

The Clerk will not however initiate and/or represent the Council in legal actions relating to data privacy issues before the courts as this would call into question his/her independence as DPO.

**Reporting Breaches**

Currently, for serious breaches, the ICO can issue a monetary penalty notice of up to £500,000; however, under the GDPR, this could be up to 20 million euros or 4% of turnover, whichever is the greater sum.

The GDPR will introduce a duty on the DPO to report certain types of data breach to the ICO and in some cases, to the individuals affected. Also, under the GDPR, a breach is more than just the loss of data, inappropriate access to personal data due to the lack of internal controls is also deemed to be a breach.

The GDPR create some new rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act *(‘DPA’)*. These are -

* the right to be informed
* the right of access
* the right to rectification
* the right to erasure the right to restrict processing
* the right to data portability
* the right to object
* rights in relation to automated decision making and profiling.

The GDPR also requires the Council to have comprehensive governance measures in place, which have previously only been considered as best practice (e.g. data privacy impact assessments are now a legal requirement). Also, the new legislation introduces the principle of accountability, meaning that the Council as data controller must maintain records to show how it is complying with the GDPR. The Council may be required to demonstrate to the ICO that it is complying with the GDPR when processing personal data.

Under the DPA, unless an exemption applies (e.g. not using a computer to process personal data), data controllers are required to notify the ICO, explaining what personal data they collect and what they do with it; they are also required to pay the ICO a fee, used to fund most of the ICO’s work based, on their size, of either £35 or £500. Under the GDPR, there will no longer be a requirement to notify the ICO in the same way, however, a provision in the Digital Economy Act 2017 means it will remain a legal requirement for data controllers to pay the ICO a data protection fee. The draft proposal is a three tier system, which will differentiate between small and big organisations and also how much personal data an organisation is processing. The aim is to keep the system as simple as possible, so that organisations will easily be able to categorise themselves. The final fees will be approved by Parliament with the proposals going live on 1 April 2018. The ICO advises that payments made during the 2017/18 financial year, under the current system, will run for a full year with the new fee becoming payable on expiry of the notification.

The appointment of the DPO does not automatically imply full compliance with the GDPR. Measures must also be put in place for the GDPR to be fully implemented in practice.

Preparations for GDPR has involved a review of the Council’s information governance practices, policies and procedures as well as ensuring the necessary technical IT and information security systems are GDPR compliant.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**RELEVANCE FOR SUTTON AT HONE & HAWLEY PARISH COUNCIL -**

*Dartford Borough Council’s Head of Legal Services has advised that Parish/Town Councils are required to appoint DPOs. Government has confirmed via the National Association of Local Councils that Parish/Town Council Clerks can be the DPO but, in order to avoid a conflict of interest, the DPO should not determine the purpose or manner of processing personal data. Members will remember that these matters were discussed and ratified by Members at the March Meeting of the Council and thereby accepting the full responsibility for the purpose and manner of processing personal data*

**Conclusion - Provided Members are satisfied that the information governance practices, policies and procedures regarding the purpose and manner of processing personal data were adopted at the Meeting of the Council held on 15th March 2018 in an open and transparent manner there should be no reason for the Clerk not to be adopted as the Council’s DPO**