THE GENERAL DATA PROTECTION REGULATION

BRIEFING NOTE & ACTION PLAN FOR COMPLIANCE BY BRENTWOOD BOROUGH COUNCIL

DECEMBER 2017

Author: Gary Cordes, Information Governance Lawyer, Brentwood Borough Council

INTRODUCTION

The General Data Protection Regulation (GDPR) becomes UK law from 25 May 2018. In due course a new Data Protection Act will effectively adopt the GDPR but with some relatively small amendments. Brexit will NOT affect the UK's obligation to comply with GDPR, so local authorities must act promptly to ensure they are GDPR compliant within seven months from now.

WHAT DOES IT MEAN FOR BBC?

The significance of the new law's effects on current data protection standards cannot be over-emphasised. With significantly increased fines for data breaches (maximum fines rise from £0.5m to £18m) and, for the first time, for other non-compliance issues, it means the GDPR represents a profound shift that will require local authorities to fully embrace the principles of data security and accessibility in a meaningful and demonstrable way. If we cannot demonstrate effective cultural as well as procedural compliance, we risk suffering a major data breach and potentially massive fines – as well as reputational harm that follows. The following represents the Council's outline action plan, sets out all the key actions required and gives some idea of the scope of the task ahead and the resource implications for the Council.

WHAT ARE WE DOING AND HOW?

The Information Governance lawyer was appointed in January 2017 to coordinate the successful operational implementation of all measures necessary to ensure compliance with GDPR by the Council. As part of the strategy, an initial appraisal was conducted of our existing DPA compliance, with a suite of new DPA policies being rolled out during Summer 2017. These, along with online DPA training for all BBC staff, were launched by the Chief Executive on our intranet system during November 2017, where all staff have been asked to read the policies and complete the DPA training by end of December 2017. Meanwhile a steering group (comprising Head of Legal, Chief Operating Officer/SIRO, IG lawyer, Head of IT, Victoria Banerji (online training provision)) and Lorne Spicer (Comms) has been established to agree our approach and, where necessary (through liaison with other senior management), to allocate work on the project.

The following represents the key elements of what we need to do to achieve effective GDPR compliance by 25 May 2018. Each element is a mini-project in its own right, highlighting the fact that proper resourcing will be at the heart of the success of the overall project and its delivery on time. These practical matters will need to be addressed early on by the steering group.

WHAT ARE THE KEY ACTIONS TO ACHIEVE COMPLIANCE UNDER GDPR?

- Appointment of a 'suitably qualified' data protection officer who may do other work for the council but that work must not compromise their ability to provide independent and objective advice/guidance to the council on all GDPR related issues
- The need to 'map' all personal data held in manual structured and electronic filing systems across the entire Council and by our partners (eg Contractors and others who may process or share the personal data we hold) including details and suitability/conformity of the systems used to process the data under GDPR
- The need to review and update our retention and disposal polices to ensure full compliance with GDPR (all departments will need to consider what personal data they hold, why they hold it, stating the lawful basis ('condition for processing') applicable, how long for and when it will be destroyed
- The need to introduce 'data protection impact assessments' (currently known as Privacy Impact Assessments) at the early stages of any proposed new contract/project involving personal data. This is a mandatory requirement in certain circumstances and fines may be imposed for non-compliance
- The need to review all of our existing data processor and data sharing agreements to ensure these and our partners/stakeholders are themselves compliant with GDPR, including a review of EVERY contract involving use of council-held personal data by external contractors since May 2016, to ensure they guarantee compliance with the new regulation.
- The need to review every one of our 'Privacy Notices' to provide the additional information required under GDPR, including an explanation of the 'condition for processing' in every case which explains why the processing is legitimate
- The need to check whether ANY personal data is obtained via consent and, if so, ensuring that the consent is provided in accordance with new GDPR requirements
- The need to update all of our existing DPA policies to make these compliant under GDPR and so 'fit for future purpose'
- The need to identify then roll out adequate training to all staff and Members and, where necessary, more specialist training to managers/senior management (we are currently working on obtaining a bespoke online GDPR training course for all staff and Members)
- The need to put in place a formal data breach policy and procedure that enables us to report breaches "likely to result in a risk to the data subject(s) to the ICO

and, where likely to "harm" individuals, to inform them too, within 72 hours of becoming aware of the data breach

- The need to ensure ongoing effective communication of all matters GDPR related, perhaps via use of a dedicated intranet page which provides a 'toolkit' comprising details of policies, training, procedures and updates on the law/other related matters affecting us
- The need to consider how GDPR affects Members acting in their capacity as individual data controllers and provide suitable guidance/training as required
- The need to ensure all new starter including contractors undertake the Council's DPA/GDPR training and read related policies as part of the Council's mandatory Corporate Induction.

At a more practical level, the following administrative and technical changes will need to be put in place, where they do not already exist:

- As above – appoint the DPO
- Annual registration (both for the Council and for Members) no longer required under GDPR but a new fees regime WILL be introduced to replace registration
- Removal of the £10 fee for subject access requests, except in some exceptional circumstances
- Ensuring our IT systems are fit for purpose under GDPR, specifically in relation to:
    1. Our ability to map all personal data we hold, as mentioned above
    2. A review of our systems to ensure they provide adequate security under GDPR
    3. Ability to comply with the GDPR "right to be forgotten" via eg pseudonymisation or anonymization if necessary
    4. Ability to dispose of individuals personal data in accordance with data protection principles (not kept longer than 'necessary').
    5. Not mandatory, but would strongly recommend we adopt a 6 month email retention policy, after which all emails will be automatically destroyed unless their content is stored securely elsewhere and where this can be justified under GDPR. This will help not only with GDPR compliance, but also where we receive costly, time-consuming subject access requests for 'everything you hold about me' without any time limitation.
    6. Other I.T. requirements/checks including cybersecurity arrangements.

This paper sets out the main elements of what we need to do. It provides a blueprint for our plan of attack in ensuring BBC's data risks are kept to an acceptable minimum as we move toward a new era of data compliance and what is now referred to as "Privacy by Design" – that is, meaningful cultural buy-in and thinking across the organisation to minimise the risk of data breach and maximise our compliance with both the letter and intention of the new GDPR.

Gary Cordes