|  |  |
| --- | --- |
| Question | Response / Comments |
|  |  |
| Can the clerk be the DPO? The Clerk would be the responsible officer too | There is nothing specific on this – the only thing GDPR (Articles 37-39) states is that the DPO:   * Have expert knowledge of DP law * Have ability to undertake GDPR tasks * May be a staff member * DPO may fulfil other tasks and duties but the Data Controller must ensure that these tasks do not result in a conflict of interests   If therefore a Clerk was to be the DPO they must have expert knowledge of DP, must have ability to undertake statutory DPO tasks and must not have other duties that may conflict their position. |
| Is there any advice/guidance on email services/providers that have European Servers would be helpful – also information on encryption. | It is difficult to give guidance as there are so many email services/providers. Its not fool proof but I would use an internet search engine and type ‘where are [insert name of provider] servers located’. I did this for gmail and did get the relevant information.  In terms of encryption the ICO does have some guidance - <https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/>  There is a free product called 7zip that can be used for encryption. This can be downloaded from the internet. |
| Regarding access requests – can we withhold negative responses or information of a private nature for example when feeding back comments around young offenders? | There are a number of exemptions in respect to data protection requests. The ICO does provide guidance - <https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/>  In this instance I would think about data protection rights of all. For example if a parent submitted a subject access request for their information and this information contained details relating to other individuals the parent would not be allowed to receive this portion of information.  You have to remember your duty of confidence and what protection this brings - <https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/> |
| Can information sourced from public sources be shared without the need for further consent? | It depends on what sources and the purpose of sharing. Generally if information is already in the public domain then it can be shared without consent.  However you have to be clear as to what role you are taking in sourcing the information. For example if you have sourced information from someone’s open Facebook page and you have sourced this as part of your job role you cannot keep going back to the same Facebook page as this is classed as surveillance and would be covered by rules under RIPA. |
| Is there a difference in the way we process data Business to Business and Business to Consumer? | The only difference under Data Protection is whether the information is personal. ICO gives you help in deciding this - <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/>  Regardless of whether its business to business or business to consumer if its personal data it falls under data protection and therefore processing has to comply with data protection requirements. |
| Is a positive action to click through a website and leave information sufficient for consent? | It would be if the click is accompanied by some text indicating what this click actually means. So if the website clearly stated ‘Click here if you consent to us sharing your personal data with [whoever]’ then this is a positive action.  Please remember that consent should not be buried in rafts of text – it should stand out to the reader. |
| Would a small Charity Company Limited by Guarantee that collects data for others as part of a contract to provide insight need to have a DPO | This link may assist - <https://ico.org.uk/for-organisations/charity/>  GDPR only states that you must have a DPO if you’re a public authority (which you are not) or if you are processing lots of personal data or special category (sensitive) personal data. Unfortunately it does not define what it means by lots.  If you are providing services for others under contract then you are probably acting as a data processor so therefore the people contracting you should be ensuring your obligations are being met. |
| What constitutes large amounts of data | Really sorry but there is no answer to this – this really comes from case law. There are some pointers though – for instance the ICO would state that if you lost more than 100 records you would be more likely to report a data breach to them.  I think you first need to understand if you data falls under the special category or not as smaller volumes of special data would concern the ICO as opposed to the same volume of standard personal data. |
| I would also like advice on how this applies to Neighbourhood Plans specifically as this is one situation in which it is normal to collect names and contact details of people commenting. My other query is do we have to apply the GDPR to data we already hold or is it data we collect going forward? | I would look at the following:   1. Can the Neighbourhood Plans work be achieved without collecting identifiable personal data? If so do not collect this data 2. Consider what is the minimum information you need to collect for the stated purpose 3. Consider your legal basis for sharing – are you obtaining consent, completing a contract, etc. The list of legal reasons are in article 6 and 9 of GDPR (currently schedule 2 and 3 of Data Protection Act) 4. If you are not relying on consent you still need to provide individuals with a privacy notice which currently tells them why you are collecting the data and who you might share it with.   Your other query is a difficult one but I think unfortunately you do have consider data already held. Hopefully most will be ok as for instance the need to have a legal basis to process personal data is a requirement of DPA 1998 already so this should not be something new for GDPR. |