The Information Commissioner's Response to the Rogue Landlord Database Reform: Widening Access and Considering the Scope of the Database of Rogue Landlords and Property Agents – closing date 12 October 2019.

The Information Commissioner is responsible for promoting and enforcing data protection law in the UK including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). She is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. She does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Commissioner welcomes MHCLG's prior engagement with us on this initiative and now the opportunity to provide a response to the formal consultation. We have reviewed the consultation paper and identified that the specifics of many of the questions fall outside of the scope of the Information Commissioner's regulatory remit. However we do have some comments in relation to data protection and privacy considerations and therefore we have set these out below, rather than by responding directly to the consultation questions.

The Information Commissioner recognises the importance of maximising the utility of the database for both tenants and local authorities. However it is important to acknowledge that the database involves personal data and

therefore any widening of access and scope to the database will need to comply with the data protection principles under the GDPR.[1]

Widening access to the database – The data minimisation principle.

The GDPR sets out seven key principles which should lie at the heart of any approach to processing personal data. Article 5(1)(c) specifies that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

The commissioner acknowledges that there are a variety of positive reasons for allowing tenants and potential tenants access to information about whether a landlord is subject to a banning order. However careful consideration needs to be given to exactly what information tenants should be given access to. Tenants should only be given access to information that is necessary and proportionate in relation to the purposes to be achieved. Not all the information that local authorities have access to may be necessary for tenants to access.

It is also noted that question 10 of the consultation asks who else may benefit from access to the database. The same points we have made above would apply here. Providing access of the database to other individuals would need to have a clear purpose and would need to be necessary and proportionate to that purpose.

Accessing the landlord/agents address

Question 12 of the consultation asks whether a redacted version of the landlords/agents address should be viewable to tenants. This is an issue we have raised concerns about in previous discussions and links into the data minimisation points we have made above. In some circumstances the landlords address could be their personal residential address. Providing a street name/partial postcode increases the risks of identifying exactly

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

where a landlord lives, especially if it is the only house within a particular street/postcode and as such would be personal data. If tenants were able to establish from the information where a landlord lives, this could present potential risks to tenants, landlords and anyone else who lives at the landlords address (e.g. in the case of a dispute).

We do have concerns whether it is necessary and proportionate for tenants to have access to the landlords address in order to achieve the specific purposes that have been set out (i.e. establish if a landlord is subject to a banning order). As we have outlined in previous advice to MHCLG on this issue, if the address is purely for verification purposes, it is our view that it shouldn't be the responsibility of the tenants to verify the identities of the landlords in question. We believe there are alternative solutions that would still achieve the intended purpose but reduce the risks to both the landlords and the tenants. For example an application programming interface could mean that very little information needs to be 'accessed' by the tenant's, instead it is cross checked in the background, yet the outcome for the tenant still achieves the intended purpose.

Access Portal

In terms of access to the database, any access should be limited to what is necessary and on a need to know basis. The risks and privacy implications could be significantly increased if the database was made public for anyone to access. This is something we discussed previously with MHCLG in earlier consultation and it is reassuring to see that MHCLG are proceeding with an access portal. However, careful consideration needs to be given to how the access portal will be managed. If it is the intention that only tenants and perspective tenants should access the portal (as the consultation describes), the information that is collected upon sign in will need to be sufficient and adequate enough to ensure that this is the case. For example if individuals were just required to provide an email address, will this mean that anyone could realistically gain access to the database? There will need to be measures in place to mitigate any malicious access to the information

within the database and ensure that those accessing the database have a genuine need and purpose for doing so. For example will there be any verification process that takes place to check that those requesting the access are genuine and not malicious?

In addition to this it is not clear whether the intention will be to allow one off access to the database or continuous access. If it is continuous access, will there be any cut off point, for example when someone buys a house and ceases to be a tenant will they still be able to access the database? These are all potential privacy risks that should be considered as part of a thorough Data Protection Impact Assessment (DPIA).

Details of the offences a landlord or agent has been convicted of

Questions 20 onwards relate to the detail of offences the landlord or agent has been convicted of and the widening the scope of the database. As outlined above it is not within the commissioners remit to specify what information should/shouldn't be viewable within the database. Any additional information that is included within the database must be relevant, necessary and proportionate in relation to the specific purposes and aims to be achieved. In this instance, the addition/widening of any offence information within the database will need to give particular consideration to Article 10 of GDPR (which relates to the processing of personal data relating to criminal convictions and offences).

Retention

GDPR specifies that you must not keep data for longer than it is needed for. Ensuring that you erase or anonymise personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping controllers to comply with the data minimisation and accuracy principles, this also reduces the risk that controllers will use such data in error – to the detriment of all concerned. It is important that in considering retention that due regard is given to the

requirements under other legislation, for example the Rehabilitation of Offenders Act 1974 (ROA). Question 22 on the consultation specifies an intention to maintain a record on the database in line with ROA but asks for further details to be provided if it is felt the timeframe should be different and asks specifically how long the landlord should remain on the database. Whilst the GDPR does not set specific time limits for keeping data, any retention should be necessary, proportionate and in line with the specific purposes for which the data is being processed. From a data protection perspective, there would need to be a strong justification and evidence basis to retain information beyond the timeframe set out in the ROA. It is our understanding that there are exceptions under the ROA, where information can be kept longer, but there needs to be a clear necessity argument set out for this.

In addition question 42 also asks whether local authorities should retain access to information held on the database after it is no longer available for tenant access, for specific purposes such as legal and/or audit? Again the same points highlighted in the paragraph above would apply here in terms of necessity and proportionality. Authorities would also need to ensure that they could identify an appropriate lawful basis under Article 6 and additional condition under Article 9 for retaining the data as well as having regard for Article 10. There is also the consideration of whether the data could be used in an anonymised form for audit purposes?

In relation to retention, it is also important that ongoing reviews and testing of the retention periods are undertaken by using available data to test how useful it has been to keep these records for the specified time. For example if records haven't been useful within 2/3/4 years then it is likely to be deemed excessive to retain them for this long.

Privacy information

The requirement to provide privacy information to individuals in relation to how their data will be processed is a fundamental right under data

protection legislation. This is an obligation that data controllers will need to comply with regardless of the lawful basis for processing (unless a restriction applies) and data should not be processed in a way which data subjects would not reasonably expect. It is important that landlords are provided with clear and informative information about how their personal data may be accessed and who will have access to it.

It is often most effective to provide privacy information to individuals using a combination of different techniques, including layering. Careful consideration should be taken regarding which format is the most appropriate under the circumstances, the provision of this information can be adapted to how information is collected. The Information Commissioner recommends that the ICO guidance on privacy information be adhered to in order to ensure that individuals are fully aware of how their data will be processed.

Data Sharing

Finally it is worth mentioning that the Information Commissioner is currently updating her Data Sharing Code of Practice (the code) to reflect changes in data protection legislation; it will also explain new developments to take into consideration. The Code has recently been published for consultation. The aim is for the code to be laid before Parliament and become statutory later in the year. Due regard should be given to the code when developing a multi-agency approach to services and data sharing.

Adhering to the code will help to ensure good practice around data sharing and help to manage risks associated with sharing large volumes of sensitive data. Following the code and adopting its practical recommendations will help to give organisations confidence to collect and share personal data in a way that is fair, transparent where appropriate and in line with the rights and expectations of the people whose information is being shared.

Many thanks for this opportunity to comment.

Information Commissioner's Office

11 October 2019