GDPR

Covid-19 briefing note: May 2020

This series of briefings address significant issues that are emerging in the UK as a result of Covid-19 that impact on the work of community investment. In each one, we have brought together available evidence to help you think about and plan future strategies and how resources can be directed. This briefing covers GDPR.

The current situation

In light of the current coronavirus pandemic affecting communities across the world, questions have been raised around the sharing of personal details, in particular of those in need of support.

This is particularly relevant to community investment professionals, both for the short-term, but also as they look to develop medium to long-term solutions based on digital provision.

For data that people have provided, this is likely to be covered by one of the following legal basis for processing;

- Consent
- Contractual
- Legal obligation
- Vital interest
- Public task
- Legitimate interests

Sharing data with other agencies

When it comes to sharing this data with other agencies who are carrying out or coordinating services, it may be prudent to be slightly more formal in approach. This will help weigh up the relevant processing basis against the interests of rights and freedom of the people in need of support in these challenging times.

Avoid sharing any unnecessary, especially sensitive or confidential personal information (termed as *special category* data by ICO).

Where possible, **set up a data sharing agreement with partner agencies.** This will help reinforce information management processes.

Data sharing agreement templates that you can use can be found in the ICO Data Sharing Code of Conduct.

Carry out a data protection impact assessment (downloadable here) before you begin any new or amended project that may involve processing personal data on a larger scale. This will help identify and mitigate against the data protection risks of any programme of work.

Please also note that the ICO is not looking to take regulatory actions against any organisation for a slight dip in standards.

Current GDPR guidelines **should prove no barrier** to you carrying out your work in the best interests of your community members.

By documenting what data they are sharing, how this will be shared, and for what reasons, you will protect yourselves against any needless worry.

GDPR

Remote working

Remote working may move data processing into a high-risk category, requiring a Data Protection Impact Assessment under the GDPR legislation. The following elements of remote working must be managed to ensure your organisations does not increase its potential data security vulnerability:

- **Policies**

  Remote working should not mean that existing organisational security does not apply, and all Information Technology and Management policy and systems administration procedures should be followed. Were changes to these are required, management should be informed, and policies updated to account for prolonged remote working where possible.

- **Video conferencing**

  Ensure that video conferencing software is used in secure manner and organisational wide guidance is given on pre-approved service providers and procedures to avoid digital eavesdropping.

- **Personal equipment**

  Employees may be using their own devices while offsite, and if so, organisations should ensure that employees have their remote hardware and work space risk assessed, and all equipment up to date with appropriate anti-virus software, firewalls and encryption as required to ensure safety and integrity of network. Guidance should also be provided over access and storing of organisational data, particularly where this contains personal information.

- **Digital signatures**

  Biometric data including digital signatures (and facial and fingerprint recognition) is also deemed personal data that relates to an identifiable person, and where being stored or used remotely, must be used in accordance with organisations data protection guidelines and agreements.

- **Scams**

  Guidance issued by the National Cyber Security Centre (NCSC) has reported an increase of scams during lockdown, with criminals primarily targeting people with Covid-19 related "phishing" emails. It is important therefore that staff remain vigilant and only open attachments or give details to trusted sources.

Tracking

The ICO is working with UK Government to ensure the safety and security of the public in the roll out of COVID tracking or analysis. Generalised location data trend analysis is helping to tackle the coronavirus crisis.

Where this data is properly anonymised and aggregated, it does not fall under data protection law because no individual is identified.

Data will be anonymised and aggregated in order to ensure no individual can be individually identified.

Breaches

Although the ICO approach during the pandemic may be more flexible than previously, and action is unlikely where requests are not satisfied within normal timescales, it remains important for any breach of data to be notified to the regulator within the requisite 72-hour period.

GDPR

Remote working (continued)

- Paperwork
  Physical documents taken off-site must also be restricted to ensure unnecessary risk is not taken, and how these would be stored or destroyed whilst staff working remotely.

Freedom Of Information

All public authorities are still encouraged to proactively publish information that they know will be of importance to their communities in accordance with FOI act, however the ICO have noted this period may contain circumstances where organisations have no option but to temporarily reduce elements of their information access functions. In order to protect against future scrutiny, the importance of proper record keeping at this time continues to be paramount.

Health data

The General Data Protection Regulations allow information on health to be shared as long as it is being done so in the interests of health and care data, including the care and treatment of patients and public health

Please feel free to contact Michael McLaughlin at HACT who can discuss the contents of this briefing in more detail and point you in the direction of appropriate online resources.