Information Security and GDPR

LARD: GDPR for research data support staff:
How can we help researchers to comply?
LSHTM, 2017-11-17

LSE Library Services
British Library of Political and Economic Science

Laurence Horton,
LSE Library

GDPR sanctions

- Written warning
- Data protection audit
- 20,000,000€ or up to 4% annual worldwide turnover
  - consent
  - data subjects' rights
  - transfers of personal data

Personal data

- Best way to manage personal data: don't collect it unless necessary.
  - Name, identification number, location data, online identifier*
  - Race or ethnicity
  - Trade union membership
  - Religious or philosophical beliefs
  - Political opinions
  - Health
  - Sex life
  - Criminal record†
  - Genetic
  - Biometric
    - GDPR, *Article 4(1), Article 9(1), †Article 10

Information Security classifications

Access levels based on ‘least privilege’ principle.

- Confidential
- Restricted
- Internal Use
- Public

Source:
https://info.lse.ac.uk/staff/Services/Policies-and-procedures/Assets/Documents/infSecStaIT.pdf

- Controlled
- Safeguarded
- Open data

Source:
https://www.ukdataservice.ac.uk/manage-data/legal-ethical/access-control

Five safes

Safe…

Projects: appropriate use?

People: researchers trusted to follow procedures and use data properly

Settings: security arrangements prevent unauthorised access or loss

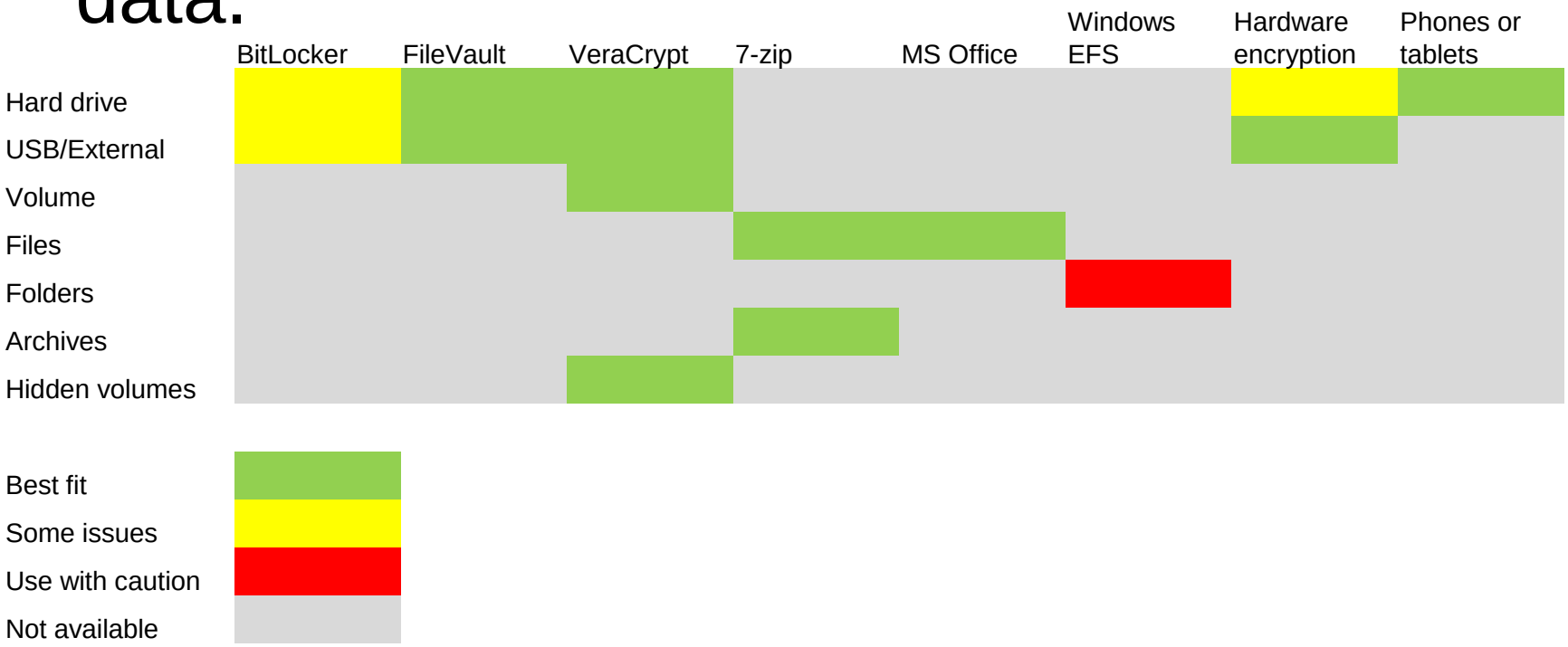
Data: Is there a disclosure risk in the data itself?

Outputs: Publications don’t contain identifying results

Source: Ritchie, Felix (2008). "Secure access to confidential microdata: four years of the Virtual Microdata Laboratory" (PDF). Economic and Labour Market Statistics. 2:5: 29–34. http://www.ons.gov.uk/ons/rel/elmr/economic-and-labour-market-review/no--5--may-2008/secure-access-to-confidential-microdata--four-years-of-the-virtual-microdata-laboratory.pdf

Encryption

- If it is necessary, anonymise it as soon as possible. Separate and encrypt personal data.



LSE Encryption matrix: http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/encryption-matrix.pdf

Physical access

- Don’t forget the physical: control access to rooms and storage.

Information Security guidance

- Check contractual requirements
  - ISO27001 (formal or ‘aligned with’)
  - Data must not be accessed remotely
  - Strong access controls (password complexity & expiry, folder access, server access)
  - Data must be encrypted
  - Secure deletion

Information Security guidance

- Warn about breaches
  - Phishing
  - Spoofing
  - Malware/ransomware
  - Theft

Information Security guidance

- Cloud storage
  - LSE has SharePoint, OneDrive
  - data held in EU (Dublin and Amsterdam)
  - accounts for external users to access where needed
  - Information Security team can assess Cloud storage providers contracts

Contact

- datalibrary@lse.ac.uk

@laurencedata

Slide notes

2. Some of the escalating sanctions GDPR can apply. If nothing else these figures are great for grabbing senior management attention. The figure of 4% is about £1.2m for LSE. GDPR strengthens rights to informed consent being sought, how data is stored and secured, and how it is shared and moved.

3. Building in “Privacy by Design”. Ask, do you really need this data? How easily can it be separated from a data set? GDPR definitions of personal data are based on what’s in the UK Data Protection Act (1998), with the addition of genetic and biometric data and an expanded definition of individual’s identity, especially digital – IP, email, social media names. Criminal record data is actually moved to a separate article with stronger protection requirements than the 1998 UK Act.

4. Working on a “Need to know” approach to data access. It’s worth attempting to identify what counts as sensitive data. Your institution may have its own information security classifications. If not the UK Data Service also has ones.

5. Much of Information Security is about policies and procedures as it is about tools. Another good reference to keep in mind is the ONS/UKDA concept of “Five safes”. Is the project proportionate to the data collected – for example, do people’s sexual orientation need to be in a study about people’s attitudes to the weather? Do people have appropriate training on how to handle the data? What security is in place – what’s the weakest link in data storage and security, for example transferring data from the field, or for transcribing or cleaning. What sensitivities are in the data itself – see information security classifications. Finally, it’s no good taking all these steps if publications and research outputs contain – either by accident or intent – identifying results. Be sure to check file metadata for any inadvertent disclosure.

6. Of course there are some tools. One questions is how do I encrypt? First thing, if possible, is to separate sensitive data if possible. Then there are different forms of appropriate encryption software depending on what needs to be encrypted.

7. One thing that can get overlooked is physical security. Who has access to rooms where data is stored, who has access to cupboards and desks where data is stored. There’s often working copies and draft copies of data that may be printed out, where are print outs left how are they destroyed? It’s worth applying a clear desk policy so nothing is left on desks while the data user is away from their desk or the room.

8. Here are some of the main issues and guidance that LSE’s Information Security team encounter and provide. These tend to relate to data acquired under licence.

9. It’s amazing how many people fall for these. They may not be related to the data itself but can compromise user accounts or networks. Be sensitive to mailbox password change emails. They try to panic people into action. There are clever spoofers out there who may try to impersonate real people associated with the university, again, don’t panic into action. Malware and ransomware can be used by hostile agencies to either compromise data or destroy it. Finally, theft or loss. We’ve all seen posters stuck up around campus pleading for return of a laptop or memory stick that contains research. If your laptop was to disappear, would your research also be gone or compromised?

10. If you have an institutional cloud then get people to use it, not google and dropbox as that could breach the transfer of personal data protection in the GDPR. If they must use them, get the data encrypted before it goes up.