Legal Aid Agency

Handling Removable Media:
A guidance note for legal aid providers

Introduction

Purpose

Legal aid providers and the LAA process large amounts of personal data every day during the course of our activities. Often, sharing personal data between legal aid providers and the LAA is essential to fulfil our functions.

As data controllers who process and share personal data, we have shared obligations under data protection legislation to adequately protect and secure the personal data of data subjects.

This guidance note will explain what these shared obligations are when personal data is shared by removable media, and how LAA providers and the LAA can work together to ensure that personal data is adequately protected.

The data protection lead or the individual responsible for data in your organisation should consider this guidance note.

What is removable media?

Removable media includes any storage device that can be removed from a computer or other device, and is used to store personal data. This can include, but is not limited to, USBs, CDs, DVDs, SD Cards, and removable hard drives.

Removable media at the LAA

Removable media is used for a variety of purposes as it can be an effective and convenient way to store and share information. At the LAA, it is mainly received from providers when providing evidence in support of legal aid applications or in claims for costs from the legal aid fund.

Data protection and removable media

Removable media, while being convenient and easy to use, must be used responsibly and in a way that is compliant with data protection legislation and requirements to protect the personal data of data subjects.

Data protection framework

Under the General Data Protection Regulations (GDPR) and the Data Protection Act 2018, both providers and the LAA must ensure that any personal data that we process is:

> *'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures' (Article 5(1)(f) GDPR)*

To be read alongside this, is the requirement that we *'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'* (Article 32(1) GDPR). Encryption is specified as one measure that can be adopted in Article 32(1)(a) of the GDPR.

The Information Commissioner's Office (ICO) have released extensive guidance relating to the security principles outlined above. Encryption is heavily cited as one measure to achieve the obligations set out in the data protection legislation. Further, the ICO have been proactive in enforcing encryption in many of their decisions in relation to data loss events in other organisations.

LAA's policy on processing removable media from providers

The LAA is currently piloting new initiatives to minimise our reliance on removable media when sharing personal data. These new initiatives will allow for data to be shared digitally through mechanisms such as Secure File Exchange (SFE).

To ensure that the personal data is protected in line with data protection and ICO guidelines in the meantime, **no items of unencrypted removable media should be sent to the LAA.** All removable media should be sent to the LAA in compliance with the Data Security Requirements, which has a mandatory requirement that all removable media must be encrypted.

Owing to the importance that removable media has in some areas of legal aid operations, the LAA will continue to accept and process these items, along with the applications and bills that they relate to. However, due to the risk to the data due to loss, theft or unauthorised access when being sent through the post unencrypted, the LAA will **not be able to return these items in an unencrypted state through the post or DX.** The legal aid provider will be required to organise and facilitate a data protection compliant way of transferring these items back to them. LAA providers can do this by:

- Organising a point to point courier to transfer the items between locations; or

- To personally collect the items from the LAA office that they were sent to.

Unfortunately, indefinite storage of this unencrypted data is not possible, therefore the legal aid provider will have a period of 28 days from the date their application or bill is processed to arrange for the return of the removable media in line with the process above. After this period, the LAA will securely dispose of the items of removable media to ensure compliance with data protection legislation*. Legal Aid providers have a responsibility to consider this and to make arrangements for the possibility that the items may not be returned should they decide to send the LAA unencrypted removable media items.

**The LAA may make alternative arrangements for the transfer of unencrypted items of removable media to the provider when there are exceptional circumstances*. *This will only be considered in exceptional cases where destroying the material would have adverse effects on judicial proceedings such as retrials or appeals. Please contact your Contract Manager or the Case Management Team that are processing your bill or application for further information.*

Frequently asked questions (FAQs)

Why is this policy being changed now?

The GDPR and DPA came into force in May 2018. The LAA have worked extensively to review and amend our processes to ensure compliance with data protection legislation. Since then, the LAA have been continuing work on ensuring greater compliance with data protection legislation.

I can send paper documents in the post that contain personal data, what's the difference?

The main distinction is the ability to protect the data. It is not possible to implement technical measures such as encryption to paper documents (encryption is viewed by the ICO as an easy and readily available method of protection); however, this is an expectation when processing removable media. This expectation is not only based on the availability of those protections, but is an appreciation that removable media can hold a large amount of personal data that can be extracted and altered with relative ease.

Can the LAA give any advice on what encryption to use?

The LAA have issued Data Security Requirements which specifies that removable media should be encrypted as a mandatory requirement, with the encryption used being recommended as 'AES encryption of at least 128-bit strength'. The ICO have issued guidance on encryption and the security principle https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/

How do I send the LAA passwords or decryption instructions?

It is important that these details are not sent with, written on or attached to the items of removable media, as this would defeat the purpose. The process for sending this information depends on the area of legal aid to which the removable media relates to. Most of these items are in relation to Crime Higher under the LGFS fee scheme, therefore the accompanying information should be sent through the *Claim for Crown Court Defence (CCCD)* system.
Where the removable media relates to Civil Certificated Legal Aid, then this information should be sent through the Client and Cost Management System (CCMS).
If your claim has been chosen for auditing or Peer Review, then the accompanying information will usually be sent through email, however please consult with the individual who requested the file.

Where can I get further information?

For further information, please contact your Contract Manager. If you have any queries about specific claims or bills, then please contact the Case Management Team processing the material.

Appendix one

Processing removable media process map