Legal Aid Agency

Working with others to achieve excellence in the delivery of legal aid

# Handling removable media

## Guidance for legal aid providers

August 2020

# Contents

# Introduction

## Purpose

Legal aid providers and the LAA process large amounts of personal data every day. Often, sharing personal data between us is essential to fulfilling our functions.

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

This guidance explains what these shared obligations are when personal data is shared by removable media.

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

## Types of 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. We mainly receive removable media from providers in support of legal aid applications or claims for costs.

# Data protection and removable media

Removable media is convenient and easy to use but must be used responsibly. We must comply with data protection legislation.

## Data protection framework

Under the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA), both providers and the LAA must ensure personal data 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)

Alongside this, Article 32(1) of the GDPR requires us to ‘implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk’. Encryption is specified as one measure that can be adopted in Article 32(1)(a).

The Information Commissioner’s Office (ICO) has 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 has been proactive in enforcing encryption in many of its decisions about data loss 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).

In the meantime, you must send all removable media to the LAA in compliance with our Data Security Requirements. This includes the mandatory requirement that all removable media is encrypted.

Owing to the importance that removable media has in some areas of legal aid operations, we will continue to accept it. However, due to the risk of data loss, theft, or unauthorised access when sent through the post unencrypted, we will not be able to return these items in an unencrypted state through the post or DX. You will be required to organise and facilitate a data protection compliant way of transferring these items back to you. You can do this in one of the following ways:

- organising a point to point courier to transfer the items between locations
- personally collecting the items from the LAA office that they were sent to

Unfortunately, we cannot store unencrypted data indefinitely. You will therefore have 28 days from the date we process your application or bill to arrange for its return. After this period, we will securely dispose of the 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.

We may make alternative arrangements for the transfer of unencrypted items of removable media to you in exceptional circumstances. Where destroying the material would have adverse effects on judicial proceedings such as retrials or appeals. Please contact your Contract Manager or the relevant Case Management Team for further information.

# Frequently asked questions

## Why is this policy being changed now?

The GDPR and DPA came into force in May 2018. The LAA has worked extensively to review and amend our processes to ensure compliance with data protection legislation. Since then, the LAA has 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 an easy and readily available method of protecting removable media however. It 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 has issued Data Security Requirements that recommends 'AES encryption of at least 128-bit strength'. The ICO has 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. For Crime Higher under the LGFS fee scheme, you should send it through the Claim for Crown Court Defence (CCCD) system.

For civil certificated legal aid, you should send it through the Client and Cost Management System (CCMS).

If your claim has been chosen for auditing or Peer Review, accompanying information will usually be emailed, 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

This summarises the process described on pages 4 and 5.