Legal Aid Agency

LAA – Information Security

Handling Personal Data and Documents

Data Security Requirements

November 2020

AMENDMENT POLICY

This document shall be amended in accordance with the relevant LAA Contract by releasing a new edition of the document in its entirety.

Changes Made to the 'Handling Personal Data and Documents – Data Security Requirements' – April 2014

Paragraph Number	Changed From	Changed To	Comments
All			The format of the document has been improved to aid the reader.

Table of Reference Documents			The table has been updated quoting the latest versions of the referenced documents.
1. Data Security Requirements	Legal Services Commission (LSC)	Legal Aid Agency (LAA)	All references to LSC have been updated to LAA throughout the document.
	The Legal Services Commission (**"LSC", "we", "us"**) is registered as a Data Controller with the Information Commissioner's Office, in accordance with section 18 of the Data Protection Act (**DPA**) 1998 [Ref. 2]. Its Notification reference is Z6467906. This Notification sets out the purposes for which the LSC processes personal data.	The Ministry of Justice (MoJ) is registered as a data controller with the Information Commissioner Office's, in accordance with section 18 of the Data Protection Act (DPA). Ref [2]	The LAA is now an agency of the Ministry of Justice and as such the MoJ is registered as the Data Controller with the Information Commissioner's Office.

	Data Protection Act 1998	Data Protection Act 2018 [REMOVED] – "section 18 of"	Updated to reflect the Data Protection Act 2018 (subject to royal assent).
		[INSERTION] – "and the General Data Protection Regulation (Regulation (EU) 2016/679)"	Updated to reflect the General Data Protection Regulation.

	Data Protection Principles	[REMOVED]	Updated to reflect the Data Protection Act 2018 (subject to royal assent) and the General Data Protection Regulation.
		[INSERTION] Instructions regarding the processing of LAA Data is set out at Annex 1 of this document and instructions regarding the processing of Shared Data is set out at Annex 2 of this document. You shall comply with any further written instructions of the LAA with respect to processing.	To reflect the requirements of Article 28 of the General Data Protection Regulation.
		References to EU GDPR changed to UK GDPR. Some links fixed	To reflect the UK leaving the EU

2. Organisation Measures		[INSERTION] - Policies – Ref 12a – Compliance with the Current Government Security Classification system	The table has been revised to give greater clarity as to which organisation measures are mandatory. Updated to include the Government Security Classification system introduced in April 2014.
3. Technical Measures		[INSERTION] - Testing and Assessment - Req. 24- Conduct independent penetration testing – Recommended.	Independent penetration testing of systems that store process or transmit information relating to 100,000 or more identifiable individuals.
Annex 1 – Processing of LAA Data			This annex has been added to reflect the requirements of Article 28 of the General Data Protection Regulation.
Annex 2 – Processing of Shared Data			This annex has been added to reflect the requirements of Article 28 of the General Data Protection Regulation.

REFERENCED DOCUMENTS

The following is a list of documents with a direct bearing on the content of this report. Where referenced in the text, these are identified as Ref. n, where 'n' is the number in the list below:

Ref.	Title	Date / Version	Author

1.	Data Security Guidance	V.2 April 2014	Legal Aid Agency
2.	Data Protection Act	2018	HMSO
3.	HMG Security Policy Framework (SPF) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf	April 2014	Cabinet Office
4.	ISO 27001	2005	International Standards Organisation
5.	ISO 27002	2005	International Standards Organisation

1 Data Security Requirements

The Ministry of Justice **(**MoJ**)** is registered as a Data Controller with the Information Commissioner's Office, in accordance with the Data Protection Act 2018 (DPA) [Ref. 2].

The Legal Aid Agency (**"LAA", "we", "us"**) is responsible to the MoJ for ensuring data is kept secure.

This Notification sets out the purposes for which the LAA processes personal data.

The LAA must receive assurances from you as one of its Providers[1] that you have taken every reasonable and appropriate measure to maintain the security of the data you will be processing on its behalf or shall be processing in common with the LAA. In order to achieve that objective, the LAA has prepared this document which sets out the basic security requirements that need to be followed, and a separate more detailed document titled Data Security Guidance [Ref. 1] which provides further information on how these requirements must be met.

In the LAA, the processing and sharing of personal data is governed by the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

[1] A 'Provider' means a party (except LAA) to a contract with LAA in respect of the provision of legal services funded by LAA

The LAA requires its Providers and any third parties appointed by Providers in accordance with the LAA contract, to comply with the Principles in order to ensure that LAA can fulfil its obligations under the Data Protection and Freedom of Information Acts.

In addition, as an Agency of the Ministry of Justice, the LAA is required to comply with the Government's minimum measures, as contained in the HMG Security Policy Framework [Ref. 3] and supporting standards, to protect personal information. This document sets a number of mandatory requirements that Government Departments and Agencies need to follow.

These requirements may change in the future as Government policies change to accommodate lessons and new developments. You must work co-operatively with us to ensure that any new obligations are complied with in accordance with the LAA contract.

For the avoidance of doubt, where you are a Provider to the LAA you are required to have regard to the LAA Data Security Requirements, i.e. this document.

The nature of the services provided by the LAA through Civil Legal Aid and Criminal Legal Aid means that clients will entrust the LAA with their personal data, which may include sensitive personal data. The LAA has an Information Charter, which provides assurance to clients that it will keep their data secure at all times.

We require LAA Providers and any third parties appointed by Providers in accordance with the LAA contract to have secure organisational and technical measures in place to protect the personal data from unauthorised or unlawful processing, accidental loss, destruction or damage and to maintain the confidentiality, integrity and availability of information.

Instructions regarding the processing of LAA Data is set out at Annex 1 of this document and instructions regarding the processing of Shared Data is set out at Annex 2 of this document. Annex 2 also sets out a description of the joint controller relationship in relationship to Shared Data.

You shall comply with any further written instructions of the LAA with respect to processing.

2 Organisational Measures

The following table shows the organisational measures that Providers should have in place. The Req. No. column is used to cross reference to the Data Security Guidance [Ref. 1] that sets out further details on how these requirements should be met.

Area	**Req. No.**	**Requirement**	**Mandatory or Recommended**	**Notes**
Governance	3	Register as a Data Controller	Mandatory	To be registered as a Data Controller with the Information Commissioner's Office, unless an exemption applies

	4	Appoint a Data Protection Supervisor	Mandatory	Appoint a senior member of staff as a Data Protection Supervisor with overall responsibility for data protection and information security
Culture	1	Foster a culture that values and protects information	Recommended	Have plans in place to foster an organisational culture that values, protects and uses information for the public good in accordance with the principles relating to processing personal data as defined in UK GDPR. This can be done through the institution of a programme of security awareness.
	6	Maintain a level of staff awareness	Mandatory	An induction plan to raise awareness to new staff on Data Protection obligations and information risk awareness and an annual training plan, as appropriate, to maintain the level of staff awareness of obligations to comply with policies and procedures.
	12a	Have a coherent set of policies	Mandatory	• Information risk management • Data Protection compliance • IT security which includes an acceptable Use Policy that outlines the type of behaviour expected from staff when using technology in the workplace and the consequences for abusing technology privileges • Compliance with the current Government Security Classification (GSC) system

Policies	12b	Have a coherent set of policies	Recommended	• Clear desk policy • Information Security, to include restricting use of portable media (e.g. USB memory sticks, discs,laptops etc) • HR standards that reflect performance in managing information risk and complying with above policies, incorporating sanctions against failure to comply

	12c	Undertake annual review	Mandatory	Supporting procedures and to conduct an annual review of the effectiveness of the policy or policies
	13	Have in place an incident management policy	Mandatory	Have a policy for reporting, managing and recovering from information risk incidents, including losses of personal data and ICT security incidents, defining responsibilities, and make staff aware of the policy
Procedures	2	Control access to personal data	Recommended	Introduce a mechanism for controlling access to personal data and restrict access to authorised staff only and restrict access to the minimum personal data necessary/relevant to job role
	5	Conduct staff screening	Mandatory	Conduct appropriate screening of staff and carrying out background checks to ensure reliability
	7	Maintain access records	Mandatory	Maintain records of staff, agents' and approved third parties' access to personal data and an audit trail of activities undertaken on it and review the audit trail for compliance with policies
	11	Conduct Data Protection Impact Assessments	Mandatory	Where appropriate, conduct Data Protection Impact Assessments of any new system developments or projects, using the Information Commissioner's guidance.
	14	Maintain adequate physical security	Mandatory	Introduce and maintain adequate physical security for premises that are used to store, process or transmit personal or sensitive information Provide secure areas for storing personal and sensitive information
	18.	Implement controlled disposal of records	Mandatory	Destroy electronic and manual records containg personal or sensitive information by incineration, pulping or cross-shredding so that reconstruction is unlikely.
	23	Implement a 'whistle-blowing' procedure	Recommended	Implement mechanisms for raising concerns about information security or any incidents of breaches of the Act or related policies.

Compliance	8.	Monitor and report	Recommended	Monitor compliance with data protection and security policies and produce annual audit report
	21.	Ensure Business Continuity	Mandatory	Create and implement business-continuity plans Create and implement disaster recovery plans

3 Technical Measures

The following table shows the technical measures that Providers should have in place. The Req. No. column is used to cross reference to the Data Security Guidance [Ref. 1] that sets out further details on how these requirements should be meet.

Area	Req. No.	Requirement	Mandatory or Recommended	Notes
Testing and Assessment	9.	Conduct formal, document risk assessments	Recommended	Conduct formal, documented risk assessments for all systems that store, process or transmit personal or sensitive information when systems undergo significant changes, or at least every 5 years
	10.	Apply appropriate controls	Recommended	Risk assessments must identify the assets, analyse and evaluate the risks to the confidentiality, integrity and availability of those assets and identify and evaluate the options for treatment of those risks. Controls and control objectives for risk treatment should be selected from Annex A to ISO/EC 27001, additional controls and control objectives may also be selected.
	24.	Conduct independent penetration testing	Recommended	Independent penetration testing of systems that store, process or transmit information relating to 100,000 or more identifiable individuals
Security	15a.	Hard disk encryption	Mandatory	All computers, including laptops, storing personal or sensitive information shall be protected by hard drive disk encryption at a minimum with access controlled by at least username and password as a mean of authentication
	15b.	Hard disk encryption	Recommended	It is recommended that the hard disc encryption product is compliant to FIPS-140 standard

	16a	Encryption of removable media	Mandatory	All portable devices (e.g. USB memory sticks, external hard drives) used to store personal or sensitive information shall be protected by using encryption
	16b.	Encryption of removable media	Recommended	It is recommended that the encryption used is AES encryption of at least 128-bit strength
	17.	Secure transfer	Recommended	Appropriate protection must be provided to protect availability of personal or sensitive information transferred from one physical location to another or transmitted electronically
	19.	Malware Protection	Mandatory	Anti-virus and anti-spyware must be installed and kept up to date on all servers, desktops and laptop computers used to store, process or transmit personal or sensitive information
	22a.	Secure disposal	Mandatory	Dispose of electronic media holding LAA Data or Shared Data through secure destruction
	22b.	Secure disposal	Recommended	If electronic media is to be reused then it should be securely overwritten or degaussed first. However, reused electronic media is still subject to the mandatory disposal requirements upon permanent disposal
Continuity	20.	Regular encrypted backup	Recommended	Back up all data on a daily basis, as required. Particular care must be taken to ensure the physical security of any unencrypted backup media

Annex 1 – Processing of LAA Data

Description	Details

Subject matter of the processing	For the LAA's purpose, to allow the LAA (and where appropriate delegated to providers) to make decisions about the grant of funding including the eligibility of the client, to monitor the progress of the matter, to make any further decisions as to case management or additional funding for the case, to make payments in respect of work done and to manage any financial contributions paid by the client or the operation of the statutory charge.
Duration of the processing	For the duration of the contract and if the case progresses beyond the contract term then for the duration of the case.
Nature and purposes of the processing	Processing by means of collection, recording, use and disclosure between the parties. You process the LAA Data as part of the LAA's statutory function that is delegated to you in order to provide legal services to LAA funded clients. Where the matter is related to a criminal prosecution then the processing will be carried out in relation to the prevention, investigation, detection or prosecution of criminal offences, in accordance with the Law Enforcement Directive.
Type of Personal Data	Name, address, date of birth, ethnicity, disability information, family members (where required) financial information (where required), facts of the case, data relating to criminal convictions (where required), medical and other expert reports (where required)
Categories of Data Subject	Clients and other parties involved in the proceedings (including respondents, experts, victims and witnesses).
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The LAA retains data in accordance with its Records Retention and Disposition Schedule https://www.gov.uk/government/publications/record-retention-and-disposition-schedules. Data will not be retained for than longer than is necessary in line with your data retention policy and the contract.

Annex 2 – Processing of Shared Data

The LAA and you are joint controllers of the Shared Data and the relationship reflects a "controllers in common" relationship as the LAA and you are both controllers of the same data although the LAA and you sometimes process it for different purposes and independently of one another.

A description of the processing of undertaken in relation of the Shared Data is set out below.

Description	Details

Subject matter of the processing	For the LAA's purpose, to allow the LAA (and where appropriate delegated to providers) to make decisions about the grant of funding including the eligibility of the client, to monitor the progress of the matter, to make any further decisions as to case management or additional funding for the case, to make payments in respect of work done and to manage any financial contributions paid by the client or the operation of the statutory charge.
Duration of the processing	For the duration of the contract and if the case progresses beyond the contract term then for the duration of the case
Nature and purposes of the processing	Processing by means of collection, recording, use and disclosure between the parties. Both parties process the Shared Data for their own purposes. You need to collect the Shared Data to enable you to act for your client. The LAA processes the Shared Data to monitor the progress of the matter and monitor the funding of the matter. For example, financial eligibility information is collected to allow you to progress the matter and so that the LAA can determine how the matter should be funded. Where the matter is related to a criminal prosecution then the processing will be carried out in relation to the prevention, investigation, detection or prosecution of criminal offences in accordance with the Law Enforcement Directive.
Type of Personal Data	Name, address, date of birth, ethnicity, disability information, family members (where required) financial information (where required), type of case, status of case, data relating to criminal convictions (where required), medical and other expert reports (where required)
Categories of Data Subject	Clients and other parties involved in the proceedings (including respondents, experts, victims and witnesses).
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The LAA retains data in accordance with its Records Retention and Disposition Schedule https://www.gov.uk/government/publications/record-retention-and-disposition-schedules Data will not be retained for than longer than is necessary in line with your data retention policy and the contract.