STAFFORDSHIRE POLICE

Data Protection Impact Assessment

"Kulpa"

Stage 2

A Data Protection Impact Assessment (DPIA) is a mandatory requirement under the Data Protection Act (2018). Publication improves transparency and can increase the public's understanding of how their information is used.

The Stage 2 DPIA has been identified as required for this project.
In this stage of the DPIA process the Project manager or Information Asset owner must provide full details about the lifecycle of the data and the risks associated with the proposal. The information provided will supplement the information provided in Stage 1.
The aim of this process is to identify and mitigate risks.

Upon completing the Stage 2 DPIA template the Project Manager and Information Asset Owner (IAO) will review, sign off and send a copy to the Deputy Data Protection Officer (DDPO). The DDPO will then seek the views of the Information Security Officer (ISO). The DPIA will also be reviewed and signed off by the Data Protection Officer (DPO). If the DPO thinks that the risks are High, then the force Senior Information Risk Officer (SIRO) will be consulted.

The SIRO may at this point ask that additional work is carried out or may decline the proposal and not accept any risks identified.

If the DPIA identifies a high risk(s) and measures cannot be undertaken to mitigate or reduce the risk then there is a requirement for the Force to consult with the Information Commissioner's Office (ICO). Consultation with the ICO will be undertaken by the Information Governance Team.

Should you have any queries in relation to the Data Protection Impact Assessment Process then please contact the Deputy Data Protection Officer at SPDPO@staffordshire.pnn.police.uk

Version	Version date	Requester of change	Summary of change(s)

DOCUMENT REFERENCES

Ref	Document Name	Version Number

Sign-Off Authority Name	Role	Date	Signature
	Senior Information Asset Owner		
	Information Asset Owner		
	Project Manager		
Information Governance sign off		**Low and Medium Risks**	
	Deputy Data Protection Officer		
	Information Security Officer		
	Data Protection Officer		
SIRO escalation		**For High Risks only**	
	Senior Information Risk Owner (SIRO)		

Section 6 - Impact
Expanding upon the purpose outlined in Section 2.1, please detail the intended effect of the processing on: Staffordshire Police; the data subjects; and society/the general public Describe the benefits and disadvantages to each of the above.
Kulpa is a new SaaS platform designed to empower victims and survivors, whilst also providing efficiency savings for policing. This in turn should reduce victim attrition and enable speedy justice. The platform is made publicly available via a free mobile app and web-app and provides a safe space to upload and securely store evidence of an offence. Then, if and when the person is ready, they can choose to report the offence via the app and share the evidence they have stored directly with the police. The relevant police force will then receive this evidence on their kulpa Police Command and Control System (kPCC) tenant. kulpa captures the available metadata associated with digital evidence at source, meaning its use should significantly reduce the need to download a victim's mobile phone or other mobile device. In effect, it enables true selective extraction of only the relevant evidence, with the victim's privacy respected and protected. To ensure that the data is secure, holds evidential weight and is legally admissible, kulpa retains two accreditations ISO/IEC 27001:2013 Information Security Management System and BS 10008:2014 Evidential Weight and Legal Admissibility of Electronic Information. The platform's automatically-populated PDF files mean that the evidence is immediately usable in an exhibited Criminal Procedure Rules (CPR) compliant format, suitable for onward transfer to the CPS for a charging decision, with minimal need for any manual processing by police officers. Kulpa was conceptualised around a systematic process-based approach which would seek to ensure that, end-to-end, the needs and requirements of each stakeholder were fulfilled to the fullest extent possible. Doing so should enable more effective and more timely justice.

Improved justice serves to improve public trust and confidence and creates an effective deterrent against committing criminal acts.

All processing is consensual under the kulpa terms, justified and The Proof of Concept (PoC) (undertaken with [redacted] demonstrated and evidenced that Kulpa could:

(a) Improve victim experiences.
(b) Save police time and/or money.
(c) Get usable data/evidence through the system more quickly.

There is compelling evidence to suggest that kulpa can empower victims and will provide considerable opportunities for efficiency savings within police forces.

Kulpa's use in the PoC resulted in a significantly more efficient, suspect-focused police investigation.

The PoC recognised a few potential barriers rather than disadvantages, namely:

It was recognised that technology is a part of life, but it does not mean everybody understands it or is able to use it, so kulpa would likely not be able to reach or help everyone.

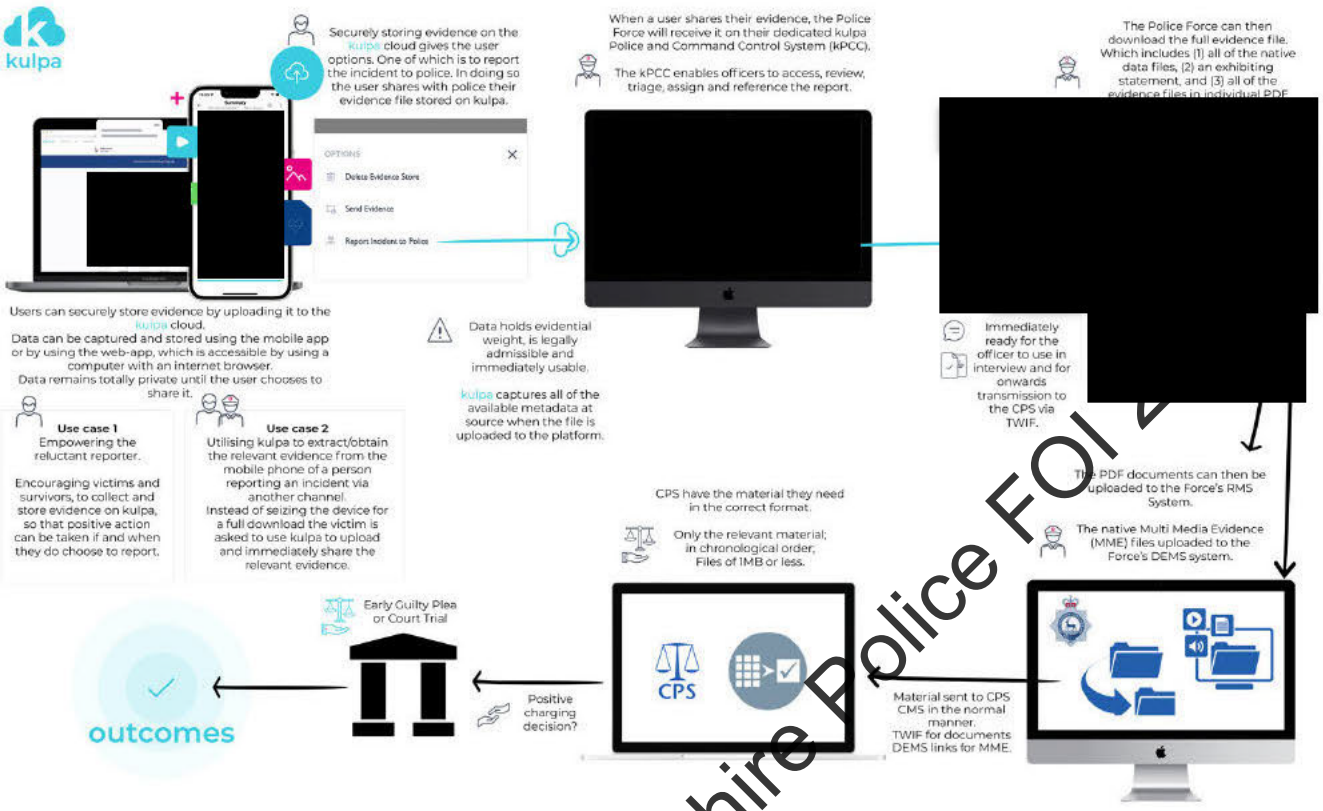
A representative from the Victims' Commissioner's office suggested that this could be a valuable tool and presents real opportunities, but in order for the full potential to be reached, and to avoid victims being disappointed, it would need to be supported by Government, Policing and the wider justice system. Another support service echoed these comments suggesting that it would need to be supported by a culture shift in policing. Another suggested that restoring confidence in police would take a 'miracle' – but seeing positive results and success over time would be encouraging.

Groups recognised "education is power" and so kulpa would need to be spoken about if people were to benefit from it.

Section 7 - Information Lifecycle

7.1 Diagrams and Tables

Please insert a diagram or table that demonstrates the flow of data within this proposal. You should reflect the information lifecycle.



[redacted]

[redacted]

7.2 Provide a full description of the information lifecycle	
Stage of Processing	**Description**
Collection Where does the data originate from, who will collect it, how will it be data obtained and how often?	A free public mobile app, encourages more victims to come forward, with a safe space to upload and secure evidence (photographs, videos, audio, messages, documents etc - all in a forensically compliant manner) and the freedom to then choose if and when to share and report. When a user does choose to share their evidence, a subscribing Police Force receive the evidence on their

	dedicated tenanted Kulpa Police Command and Control system (kPCC) which will provide a fully CPR-compliant evidential package to enable an immediate, suspect-focused investigation, without the need to seize or download the victims mobile phone.
Storage Describe where and how the data is to be stored	Kulpa stores and processes data on Microsoft Azure. UK Data is stored exclusively in UK Regions. kulpa's system runs on the [redacted] All data is stored and processed in the UK and in line with all UK policing requirements. Upon a user choosing the option to 'share with police' the data is transacted to the relevant police force on their tenanted kulpa Police and Command Control System (kPCC). Help/support videos for full details - https://www.youtube.com/@kulpaCloud/videos Data shared via kulpa is accessed by police via the kPCC system. This system is provisioned by kulpa and then access provisions are managed independently by the force via active-directory SSO. The kulpa system uses the location of the reported incident to identify which force tenanted kPCC the data is transacted to. i.e. A crime in [redacted] goes to [redacted]. Whereas a crime in [redacted] would go to [redacted] and [redacted] Data is reviewed and then downloaded from the kPCC and uploaded to the force RMS and DAMS The kPCC is accessed via any browser. https://police.kulpacloud.com/ (for those who have been provisioned SSO access by the Force) The mobile app can be downloaded from the app or play store and is accessible to anyone who registers. The public app is also available using a web browser by visiting kulpacloud.com All of the evidential packages obtained via the kulpa application are to be uploaded to [redacted] existing RMS and existing DAMS systems. The upload to the [redacted] systems is manual (a download, drag and drop if you will). Although in the future there is the potential to automate this, Kulpa provides all of the native files (multimedia evidence, photos, videos, documents etc) - these are to be uploaded to the [redacted] DAMS. Kulpa also converts all of the files into PDF files and provides Criminal Procedure Rule compliant statements, suitable for transfer to the CPS. These should be uploaded to the RMS or DAMS and then from those systems transferred to the CPS via TWIF. A change request has been put in place for the development of an API to Automatically transfer data when it is submitted into Kulpa then transferred into the DAMS environment. Which will be the long term Digital Storage Solution. The data will be transferred into [redacted] as required. Data would only be stored as per the guidelines implemented, which would be an upload to RMS and DAMS. It

	should not be stored anywhere else. Kulpa anticipate that [redacted] would assess the report via the kPCC, download the data and then transfer the case to the relevant team as per normal processes for crimes reported via, 999, 101 or SOH At this point, normal/standard processes, procedures and protocols continue. They will be retained and disclosed as per existing policies and procedures. To ensure that the data is secure, holds evidential weight and is legally admissible, kulpa retains two accreditations ISO/IEC 27001:2013 Information Security Management System and BS 10008:2014 Evidential Weight and Legal Admissibility of Electronic Information
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	See screenshots of the kPCC screens, would be logged by Staffs using the usual markers. A case would be created in MICHE and this number then entered into the kPCC to ensure that everything is linked/Matched together. [redacted] Main dashboard [redacted] Space for [redacted] Ref to be linked

[redacted]

Incident review screen

[redacted]

Further details with ability to review shared evidence immediately

The data provided from a kmpa submission will be used as evidence, to support an investigation of the reported incident and potentially a prosecution.

A reference number is entered by the reviewing police officer into the kPCC. 'An [redacted] reference'. The kmpa user will then be able to see this reference, and there case will also turn blue on their app so that they know it has been reviewed. See attached screenshot. Further contact would be made through normal channels, phone, email, face to face.

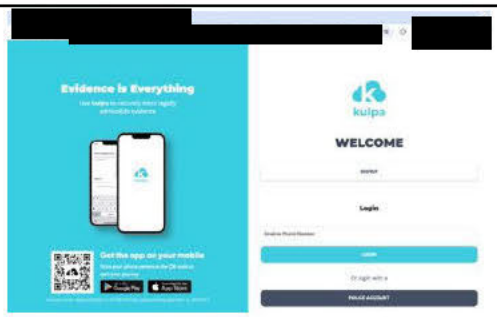
[redacted]

Reference number entered on kPCC

Once a reference number is assigned the app displays a blue icon to the user

They can also via the app see the reference so that they can contact the force should they need to moving forward.

Whilst the concept of kulpa is novel (it being a publicly available app), the technology used and processing is not novel. It is a data transfer of evidence and does not involve any other novel analysis or processing in the transaction between the kulpa platform (kPCC) and police systems.

	 Login screen to the Kpcc  Example of audit trail which is accessible to all users.
Access Describe who has access to the data throughout the life of the processing	Access to the kPCC is managed via the Forces own Single Sign-on (SSO) policies. The force therefore has full control over who can access the system, and ensures that access is provisioned and then de-provisioned when someone joins, moves or leaves. Kulpa has a full audit trail of all activities [redacted] Police, will only be able to see via our dedicated kPCC, the data which has been shared by a user reference a specific incident. [redacted] will not be able to see any information which has not been explicitly shared by a user and you will not be able to see shared data unless the incident being reported is within your force boundaries. The Kulpa user can upload more data as and when they wish to do so. If they do this post a case already having been submitted then a message stating that further information has been uploaded will be sent to those using the kPCC within the force.

Recording Describe the processes for recording the data	If a kulpa user chooses to share their information and evidence with the police, the relevant police force (being determined by the location of the incident), will have access to the information, initially via the kulpa police command and control system (kPCC) (Identity for which is managed by [redacted]. A crime record will then be created on the RMS and all supporting documentation and evidence from kulpa, attached to that record. Crime reference is entered into the kPCC. Evidence is transferred to RMS([redacted]) and DAMS At which point access to the data is given to anyone with RMS access. Officers can also, limit the viewing of evidence on the KPCC if it is sensitive. The system will automatically blur and sensitive photographs. All actions are recorded in the audit log. A sensitive marker can also be placed on a case. Turning this on will result in an additional check screen, asking the user if they have legitimate and reasonable need to access the record [redacted]
Processors Describe the use of processors. If a third party is being used then is a contract in place to regulate the relationship? Will the data be processed outside of the UK or the EU?	Kulpa processes users' data in-line with its users terms and conditions. These same terms enable kulpa to transfer their data to law enforcement upon the users request. kulpa processes all data internally before it is shared with policing. All of kulpa's data storage and processing occurs in the UK.

	'Policing Data' is not being processed by kulpa or any other third party. This is a one-way exchange of information between kulpa and police, as an when a kulpa user requests that their data be shared. Kulpa stores and processes data on [redacted] Data is stored in [redacted] Before using the kulpa platform (either the mobile app or web-app) the user must agree to kulpa's terms, conditions and privacy policy. The acceptance of these terms means that the user has expressly given permission for data to be shared and processed by law enforcement. This consent is then re-affirmed twice more at the point at which the user, presses the option 'share with police'. For the avoidance of any doubt, information shared by kulpa users with policing by selecting the option to 'share with police', will be received by the police force on their tenanted kulpa Police and Command Control System (kPCC). It is then for the reviewing officer / police staff to review the report, download the evidential package from the kPCC and upload it to the force RMS and DAMS systems. At this point, normal/standard processes, procedures and protocols continue. It is essentially a new method for receiving an immediately usable package of digital evidence. No procedures or processes which follow are altered in any way. The information is uploaded to the existing RMS and DAMS. It is then on these systems which it is managed and shared onwards, for example to the CPS via TWIF.
Sharing With which external organisation(s) is the data shared, what data is shared, and why?	Kulpa will share data with the relevant police force, if a user selects the option to 'share with police'. The 'relevant force' will be determined by the reported location of the incident. Officers with access to the [redacted] kPCC will then be able to access the data shared.

Describe any sharing that will occur within Staffordshire Police. Outline any national and international sharing or processing.	Data obtained from kulpa may then be shared by [redacted] with CPS and referrals to support agencies, if appropriate, as per any other recorded crime.
Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate	[redacted] all of the evidential packages obtained via the kulpa application are to be uploaded to the existing RMS and existing DAMS systems this is where they will be held for review and retention purposes. They will be retained and disclosed as per existing policies and procedures. [redacted] will follow CPIA guidelines and Forensic Science Regulator requirements with regards to data being processed and involved. [redacted] hold and retain data in line with its user terms and privacy policy. SoPs and accreditations kulpa has a full retention and disposal policy. Any data which is shared by Kulpa with police is retained for a minimum of 7 years within their system.
Disposal Describe the process for disposal of data, including when and how.	[redacted] all of the evidential packages obtained via the kulpa application are to be uploaded to the existing RMS and existing DAMS systems. They will be disposed of as per existing force policies and procedures. Following CPIA guidelines with the data involved. If a user has not shared the data file and requests via the app that it is deleted, then the system will delete it via an automated process. Data files which have been shared with police are reviewed manually after 7 years, at which time, retention or disposal policies are followed. Please note, Kulpa's retention of data is a safeguard, as the data should also already have been transferred to the force DAMS and RMS.
7.3 Assets Describe the assets that you intend to use.	
Hardware	
Software	Software as a Service (SaaS) The kulpa platform including the kulpa police command and control system (kPCC).

Networks	Kulpa Connection Requirements [redacted] [redacted] [redacted]
Hardcopy/paper	
Any other relevant assets	

Section 8 - Consultation

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you consider consulting them or their representatives.

8.1 Do you intend to consult data subjects?

☒ **Yes**

If yes then outline your plan in **Section 8.2** below together with details of consultation with other stakeholders.

☐ **No**

If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 8.2** below.

8.2 Consultation Action Log

Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- The general public
- Union representatives
- Information Security
- DPO
- Staffordshire Police Legal
- Partner agencies
- NPIRMT
- Data processors
- Information Commissioner's Office (ICO)

Who	When	How	Outcome
Data Subjects	SEPT 2025	Engagement with IDVA's	Positive
Information security	Jan 2023	[redacted]	Passed

Section 9 - Full Risk Assessment

Identify and Assess Risks

In this section you must detail **all** data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. **The assessment criteria outlined in italics in section 9.1 applies to all categories** in Section 9 and 10 i.e. for 'likelihood' you must always assess whether it is 'rare, unlikely, possible, likely or almost certain'.

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

** Please refer to *Appendix A – Calculation of Risk* for matrix used when identifying Risk Scores.

Examples of **risks to individuals** include:	Examples of **corporate risks** include:
• Discrimination • Identity theft • Financial loss	• Failure to protect the public • Loss of public confidence • Civil litigation

• Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights	• Reputational damage • Regulatory action • Breaching other legal obligations

You should identify **solutions** such as:

- Deciding not to collect certain types of data
- Reducing the scope of processing
- Reducing retention periods
- Taking additional technical security measures
- Following approved codes of conduct
- Restricting access to data
- Training staff to understand the risks
- Anonymising or pseudonymising the data
- Using different technology
- Using an alternative third party processor

9.1 Data Protection Principles

1. Fair and Lawful

- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation

- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation

5. Retention

- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all Staffordshire Police systems if required?
- Is the retention period necessary and proportionate?

6. Security

- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?

- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy

- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights

- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to the DPO.

[redacted]

[redacted]

9.2 Data Sharing - including the involvement of other Controllers and Processors	
- What contracts, MOUs etc are in place or may be required?	- What risks are involved with sharing data?

- What measures have you taken place to ensure third parties comply with Data Protection laws? - Is sharing necessary and proportionate? - Is the sharing of data being minimised?						
Describe the source of risk and the nature of potential impact on individuals, include associated organisation/corporate risk and compliance risk	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**

9.3 International Transfers

- Will data be shared with a third party based outside the EU?
- If you will be making transfers, how will you ensure that appropriate safeguards are put in place?

Describe the source of risk and the nature of potential impact on individuals, include associated organisation/corporate risk and compliance risk	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**

9.4 Additional Risk Factors

Describe any further risks, ensuring that any risks not already identified are included.

Describe the source of risk and the nature of potential impact on individuals, include associated organisation/corporate risk and compliance risk	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk

Section 10 - Operational Data Risks - Additional Risks Relevant to Operational Data Only

This section is only applicable to proposals involving operational data. **If you are solely processing administrative data then move to Section 11.**

[redacted]

10.2 Data Categorisation

When processing data for law enforcement purposes, you must **provide where relevant and as far as possible** a clear distinction between categories of data subject.

Will there be a clear distinction between different categories of personal data suspects, for example subjects who are:

[redacted]

DPO USE ONLY			
Section 11 – Outcome and Review			
11.1 Outcome			
Item	**Name**	**Date**	**Notes**
Residual risks approved by:			
DPO advice provided by:			

Summary of DPO advice, including whether the ICO must be consulted:			

11.2 Review
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live. Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged.
Outline: • Who will be responsible for reviewing the processing • The frequency of review • The date of the next review

11.3 Conclusions
DDPO Conclusions:
Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with the DPA2018. Includes references to any changes that were introduced as a result of the DPIA process.

ISO Conclusions:
Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with Information Security Requirements. Includes references to any changes that were introduced as a result of the DPIA process.
DPO Conclusions:
Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with Data Protection Act 2018 and risks to Staffordshire Police. Includes references to any changes that were introduced as a result of the DPIA process.

Annex A

Data Protection Principles

1. Fair and Lawful
- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation
- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation
- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy
- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention
- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all Force systems if required?
- Is the retention period necessary and proportionate?

6. Security
- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights

- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to Information Rights.

kulpa [OFFICIAL V1-101-F]

Phase 1 - User Feedback

The survey was run using Microsoft forms. The results are detailed below:

Does the client feel safer?

[redacted]

Overwhelmingly positive with 85% of users feeling safer as a result of having kulpa

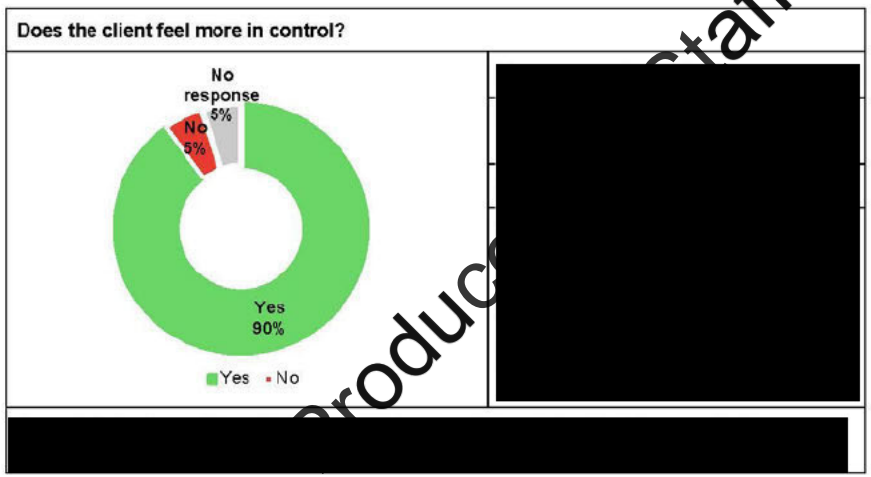
Is the client using the Webapp (website) or the Mobile App?

[redacted]

[VE
e)

kulpa [OFFICIAL V1-101-F]

[redacted]

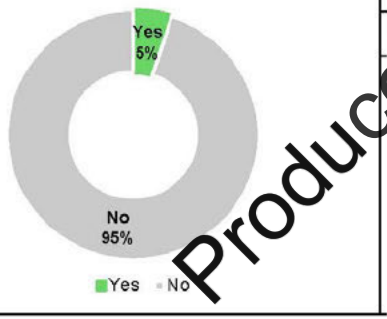


[VE
e)

kulpa [OFFICIAL V1-101-F]

[redacted]

Has the client referred their evidence to Police?



Breakdown

[redacted]

If No, why Not?

[redacted]

[VE
e)

kulpa [OFFICIAL V1-101-F]

[redacted]

[redacted]

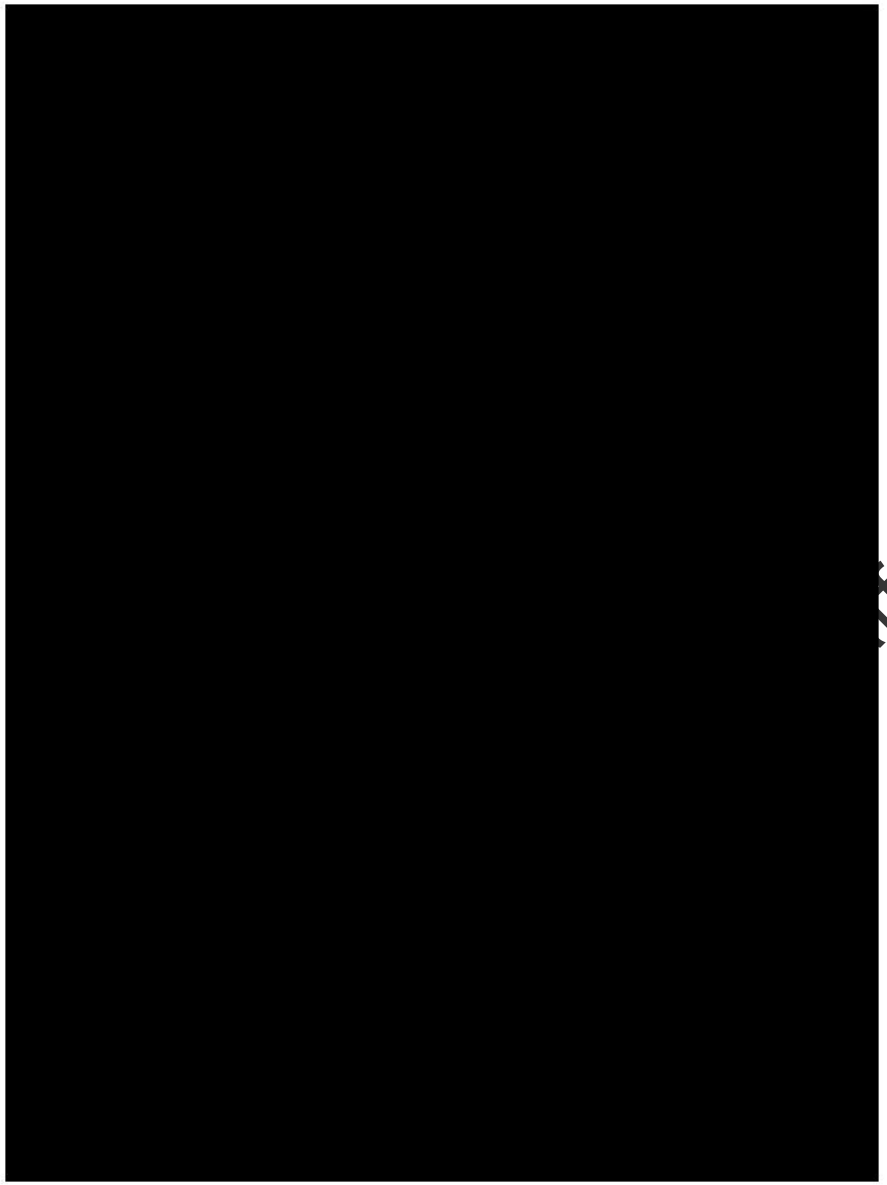
[VE
e)

kulpa [OFFICIAL V1-101-F]

[redacted]

[VE
e)

kulpa [OFFICIAL V1-102-S]

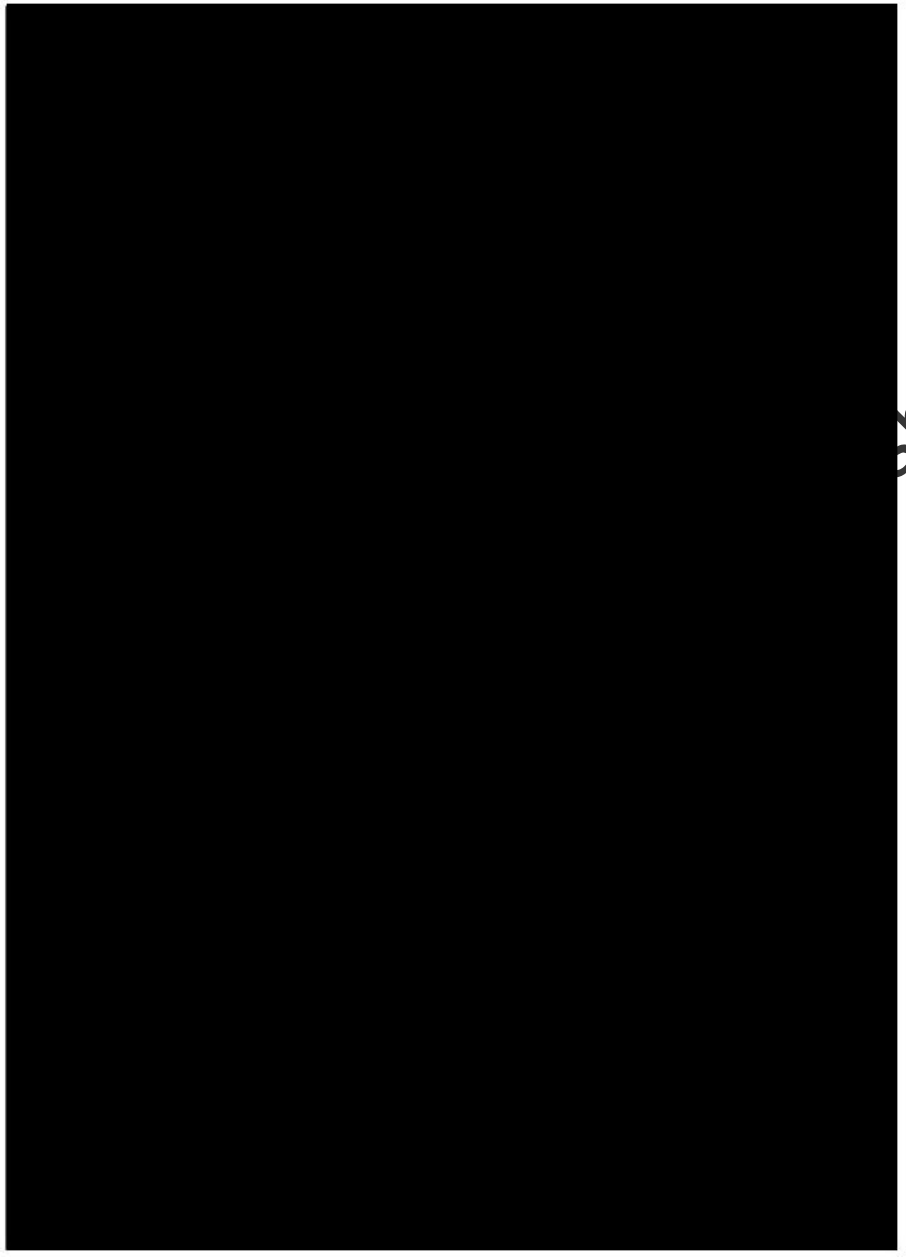


kulpa [OFFICIAL V1-101-F]

[redacted]

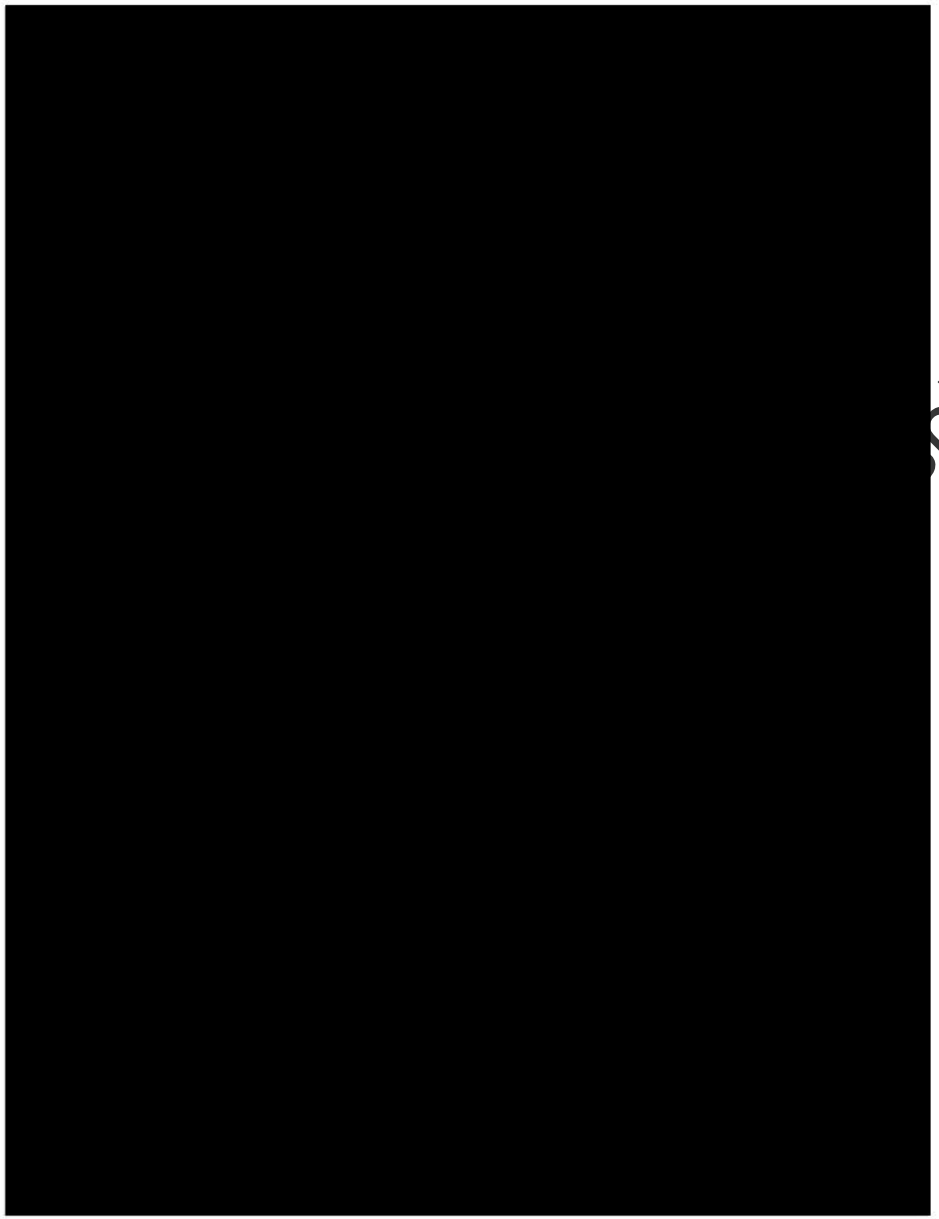
[VE
e)

kulpa [OFFICIAL V1-101-F]



[VE
e)

kulpa [OFFICIAL V1-101-F]



[VE
e)

Kulpa - technical due diligence report

[redacted], P2P Consulting & Development for Suzy Lamplugh Trust 2024-12-20

[redacted]

Executive summary

Kulpa's offering seems well-designed and the company has a good understanding of the needs of organisations such as the Suzy Lamplugh Trust and the Trust's clients. The offering is a good match to the requirements of the Trust as expressed to the author and should provide appropriate cybersecurity measures to meet these requirements.

Background

The Suzy Lamplugh Trust commissioned [redacted] or [redacted] to perform basic technical due diligence on cybersecurity aspects of Kulpa with a view to using and recommending their solution to the Trust's clients and in conjunction with the various police forces with whom the Trust works.

A summary of the kulpa platform (provided by kulpa)

"kulpa provides a free app, already available on iOS, Android or via any web browser, which empowers users (in the case of the Suzy Lamplugh Trust, victims of stalking and harassment) to securely upload their evidence to a secure cloud. The app can accept any file of any size; photos, videos, audio files, text messages, social media screenshots, whatsapp exports, CCTV, doorbell footage, documents, etc. Then, whenever the victim is ready, they can choose to share their evidence, directly from the app. Sharing can be with the police and/or with a legal representative (if a civil action is required) or indeed anyone else who the user chooses.

Kulpa has two UKAS accreditations and a unique ability to absorb, analyse and present the Meta Data associated with any files uploaded and shared. Given such, the CPS have supported its use.

When a user chooses to share their evidence with police, the kulpa platform provides the police with a CPS-compliant package of evidence which includes all of the evidential items
pre-exhibited, together with a pre-populated, digitally signed MG11 statement. This ensures a more effective and efficient, suspect focused investigation with the opportunity for improved outcomes.

KULPA empowers victims to provide the police with immediately usable digital forensic evidence, in significant quantities, without the need to have to seize or download their device. It protects and respects victims and enables suspect-focused investigations."

Scope

The technical due diligence process was to cover Kulpa's application, services and processes and to consider their appropriateness against two specific criteria:

- Victim safety;
- Evidential admissibility of information provided by victims.

Process

The due diligence process was performed under a one-way Non-Disclosure Agreement from Kulpa to P2P Consulting & Development. This report has been disclosed to Kulpa before being

shared with the Suzy Lamplugh Trust to ensure that no confidential information is disclosed, but the author asserts that no undue influence has been exerted by Kulpa to change the material findings of the report, which represents the author's professional opinion.

[redacted]

A full architecture, design and implementation review was not conducted as it was outside the scope of the engagement.

Evidence

Kulpa holds the following certifications:

- Information Security Management System - ISO/IEC 27001:2013
- Evidential Weight and Legal Admissibility of Electronically Stored Information (ESI) - BSI 10008:2020

These are key certifications for managing sensitive information and information that is intended to have evidentiary admissibility within the courts system. Certificates were provided to the author in electronic format. The supporting documentation was also provided in electronic format. Everything appeared to be appropriate and in order.

Kulpa is registered with the Information Commissioner's Office (ICO) -

verified. Information provided by Kulpa but not verified as part of the

report:

- The use of Kulpa's service is supported and approved by the Crown Prosecution Service.

- Kulpa lists multiple organisations who are using their application and services. These include a number of victim support charities (e.g. Choices, The Domestic Abuse Alliance, Refuge).
- Kulpa's CEO, [redacted], is [redacted].
- An external PEN test was commissioned by the Home Office in 2023. "The result of said test was a pass, sufficient that the Home Office were content that kulpa could be used in a 'live environment' and offered for public use." (Kulpa)

There is no reason to doubt any of the information presented above, all of which could be verified if required.

CONFIDENTIAL

3

Findings

Areas addressed included (but were not limited to):

- Use of encryption
- Cloud provider
    - Choice of cloud provider
    - Jurisdiction in which cloud provider operates
    - Cloud provider staff access to information
- Mobile device security
- Data protection at rest
- Data protection during transport
- Data protection in use
- Ongoing reviews and penetration testing
- Service software and hardware architecture
- Kulpa employee/staff access to information

Based on the evidence provided and discussions undertaken, Kulpa has a good understanding of appropriate security measures in the two areas of most interest to the Suzy Lamplugh Trust: victim safety and evidential admissibility. The architecture and design of its system take into account best practices in the industry and show appropriate measures, technical decisions and choices to support these areas. Choices around the cloud service used and implementations also seem appropriate.

Recommendations

A small number of technical recommendations were made by the author of the report under the Non-Disclosure Agreement for consideration by Kulpa, none of which are considered urgent, but which might improve the service in the future. These were warmly received by [redacted] and one of them is already being implemented. Others are under consideration for future work.

The author does not believe that there are any outstanding technical issues that require implementation at time of writing in order to support the aims of victim safety and evidence admissibility.

Conclusion

Kulpa's offering seems well-designed and the company has a good understanding of the needs of organisations such as the Suzy Lamplugh Trust and the Trust's clients. The offering is a good match to the

requirements of the Trust as expressed to the author and should provide appropriate cybersecurity measures to meet these requirements.

CONFIDENTIAL

4

[redacted]