Philip Seccombe
Police and Crime Commissioner
for Warwickshire

DATA PROTECTION IMPACT ASSESSMENT

OPCC CASEWORK SYSTEM

18th August 2020

Office of the Police and Crime Commissioner for Warwickshire

Details of project/change

Project name	OPCC Casework System
Brief description of project/change	Introduction of a cloud-based ICT software solution (known as Caseworker.gov) for the management and resolution of correspondence and casework undertaken within the Office of the Police and Crime Commissioner (OPCC) for Warwickshire
OPCC Lead	Richard Long
Name of Data Protection Officer (DPO)	Warwickshire Legal Services
Target date for implementation of project/change	November 2020
Date	18th August 2020

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Currently all correspondence received by the OPCC and all casework undertaken by staff, is managed and resolved in a disparate and fragmented way through the use of a range of storage folders on the local ICT network and spreadsheets to track and record progress and outcomes. This is not an effective and efficient solution and makes it extremely difficult to ensure that the requirements of the General Data Protection Regulations (GDPR) are adhered to. The purpose of the project is to implement the use of a cloud-based software solution known as 'Caseworker.gov' developed by Elected Technologies Ltd; in order to replace the current arrangements, resolve the identified issues, and ensure compliance with GDPR and Data Protection requirements. Please see attached Business Case:  Business Case for Case Management S A Data Protection Impact Assessment (DPIA) is being completed in order to systematically and comprehensively analyse data processing in relation to Caseworker.gov and help identify and minimise the data protection risks of the project. Although low volume, the OPCC does sometimes find itself processing data that may result in high risk to individuals and from that perspective a DPIA is a legal requirement. However aside from this, a DPIA is being undertaken as good practice as the project requires some processing of personal data and its completion can bring broader compliance, financial and reputational benefits, help to demonstrate accountability, and build trust and engagement with individuals.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Please refer to the attached Record of Processing Activities (RoPA) which sets out all of the OPCC's processing activities including who data is shared with. Additionally, please refer to the OPCC's Full Privacy Notice and associated Appropriate Policy Document (APD) as required under Schedule 1 of the DPA 2018 in relation to the processing of special category and criminal offence data. Public-facing versions of the Full Privacy Notice and APD are published on the OPCC website:


Record of Processing Activity (I


Full Privacy Notice (Update 13.08.20).pd


Appropriate Policy document OPCC Jul

Additionally, the attached OPCC Processing Workflow document sets out the nature of the processing including the source of data received by the OPCC, what it relates to, how it is received/collected, how it is routed and by whom it is actioned:


OPCC Processing Workflow.xlsx

Incoming correspondence received into the 'OPCC Warwickshire' group email inbox will automatically be redirected into the inbox of Caseworker. Emails received into other group inboxes (such as 'OPCC Grants') may also be set for automatic redirection, or alternatively relevant emails from those inboxes may be forwarded manually. Likewise, relevant emails received into the individual email inboxes of OPCC Staff may also be forwarded manually into the inbox of Caseworker.

Once email correspondence has been received into Caseworker it will be listed in the systems own inbox. From here unwanted emails can be deleted. However, individual or groups of emails that require action can be used to open a 'Case' file. During the process of opening a 'Case' the origin emails will be attached to the file and the 'Case' will be ascribed a range of detail from drop-down or free-text fields, which will include the 'Origin', 'Type' and 'Subject' matter.

As the above Processing Workflow document shows, the vast majority of correspondence received by the OPCC is via email. However, it is not the only route in which correspondence is received and/or casework is required and other routes include receipt of hard-copy letters, contacts via the OPCC Website and Social Media accounts, telephone calls, issues raised in public meetings, along with verbal/written tasks arising out of the Police & Crime Plan or for other priorities (such as Public Consultations), etc.

Consequently a 'Case' can be opened directly within Caseworker without the need for a source email. Relevant copies/scans of papers or other documents can be uploaded to the 'Case' file and in exactly the same manner as before, the 'Case' will be ascribed a range of detail from drop-down or free-text fields, which will include the 'Origin', 'Type' and 'Subject' matter.

Elected Technologies has stated that all data held within Caseworker is stored and processed electronically within Google's EU data centres. Historically this has been in Belgium and London, but with the advent of the UK leaving the EU, Elected Technologies have made a conscious decision to move all data stored in relation to Caseworker into Google's London data centre only.

The provider has a single third-party processor that is legally based outside the EU that they use for outbound transactional emails only, and their data processing with them has historically been covered by a specific data processing agreement, the EU/US Privacy Shield and GDPR EU approved Standard Contract Clauses (SCCs).

The OPCC's contract with Elected Technologies will include EU approved SCC's so as to provide adequate legal safeguards in relation to any data that is transferred outside the EEA, in compliance with DPA 2018 (see section on 'Context' – page 4). The parties will contract under the CCS G-Cloud framework and the OPCC will provide written instructions to Elected Technologies (who are a data processor under this arrangement) by the adoption of a data processing schedule.

Update in relation to the Schrems II case

Both this DPIA and Elected Technologies recognise the impact of the Schrems II Judgement, which has just invalidated the EU/US Privacy Shield. The question now arises as to whether the European Commission/Information Commissioners Office (ICO) consider Standard Contract Clauses to be sufficient protection on their own, or whether further measures such as additional technical encryption is required. Further work is underway nationally to provide more comprehensive guidance on any extra measures that may need to be taken, however the current advice from the ICO is that we should take stock of any international transfers made (in this case by Caseworker.gov) and react promptly to that guidance and advice as and when it becomes available. Separately this is described as conducting an assessment as to whether Standard Contract Clauses provide enough protection within the local legal framework.

As part of implementation of Caseworker.gov and for this DPIA specifically, due diligence has been undertaken with Elected Technologies regarding the Schrems II judgement. Elected Technologies have themselves sought legal advice. The position currently is that, having reviewed the judgement, the advice from their legal advisors, and with the specific contracts and data protections agreements they have in place (which already incorporate Standard Contract Clauses), they are confident that there is sufficient protection in place to meet GDPR requirements for the transfer of data within the context it is taking place.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The OPCC recognises that having accurate and relevant information is essential to effective decision making and that good records management enables business to be conducted in an orderly efficient and accountable manner. There are inherent risks attached to the retention and disposal of records which directly affect public confidence, legal issues and complaints legislation.

Consequently the OPCC has in place the following attached 'Records Management Retention and Disposal Policy'. This policy and its related 'Retention Schedule' provides the OPCC with a common and consistent approach to the retention and disposal of records that seeks to balance proportionality and necessity, which will apply to data held within the Casework System:


FINAL Records Management and R


FINAL Retention Schedule 04.12.19.p

In proportion to the small number of operational staff within the OPCC for Warwickshire, the volume of correspondence/contacts received is high (approx. 2,300 per year). However, from a holistic perspective the total volumes are very small in comparison to other organisations. In addition, not all of those correspondence/contacts contain personal data that will be processed through the Casework System.

The vast majority of data to be processed through the Casework System is individually classified as fairly 'low risk' under GDPR. The OPCC does occasionally find itself processing Special Category and/or Criminal Offence data, but usually not in large volumes so as to be classified as 'high risk' by volume under GDPR.

However, given the nature of some correspondence/contact, the OPCC also occasionally finds itself processing data that might endanger the individual's physical health or safety in the event of a security breach. In many cases this data has been willingly provided by the individual to the OPCC as part of their communication, but they have mistakenly believed they are providing it to Warwickshire Police (a separate organisation). In those cases the individual is re-directed to the Police and any 'high risk' data is immediately deleted. In other cases where it is necessary for the OPCC to retain such data in order to undertake further activity, this is done in accordance with the aforementioned GDPR-compliant 'Records Management Retention and Disposal Policy' and 'Retention Schedule'.

The Casework System supports this policy and GDPR compliance by allowing a full and accurate search against all 'Cases' and their fields. It also automatically attaches a data 'Deletion Date' that reflects the type of case and subject matter.

At all times, in line with GDPR, the processing of data with be minimised as far as possible and there will be no unnecessary duplication or replication of data either held within the Casework System or held elsewhere. As part of the implementation of the Casework System a clear procedure will be created that sets out the expectations regarding what data is held 'within' and what sits 'outside' the system.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Police and Crime Commissioners (PCCs) are directly elected representatives of their local communities and were elected for the second time on the 5th of May 2016 in 40 police force areas across England and Wales. Every force area is represented by a PCC, except Greater Manchester and London, where PCC responsibilities lie with the Mayor.

The role of the PCCs is to be the voice of the people and hold the Chief Constable to account, effectively making the police answerable to the communities they serve. To support them in this role each PCC has a team of staff consisting of a number of roles, collectively known as the Office of the PCC (OPCC). In relation to the role and remit of the PCC, correspondence/contact is received into the OPCC and will be processed through the Casework System. These are received from both organisations and individuals, as set out in the 'source' column of the attached OPCC Processing Workflow document:

OPCC Processing Workflow.xlsx

With the exception of press releases, surveys and the carrying out or commissioning/grants processes, the vast majority of correspondence/contacts received by the OPCC are prompted by the source themselves. Such correspondence/contact is entirely voluntary and the information provided given freely. Individuals have full control of the information (data) provided, either on initial contact or subsequent communications. This data is provided by them for a specific purpose, usually in the expectation of engagement or action by the PCC or a member of the OPCC.

On occasion the information (data) can include details about children or other vulnerable groups, but where this occurs it is usually in connection to the reasons for the correspondence/contact with the PCC/OPCC.

Technology such as the Casework System are in widespread use across the public and private sector. Indeed, it is likely that any source of correspondence/contact with the OPCC will likely believe such a system is in already in use by the team. Versions of the Casework System solution being procured are in wide use across England and Wales. There are no plans to use the system in any novel way and no known current issues of public concern.

There are no concerns over the type of processing that will be undertaken within the Casework System proposed and, to our knowledge, no reported security flaws. Research has been undertake with users of the system (specifically two local MP offices) and their feedback was excellent with no reported issues, concerns or problems with compliance.

In general terms regarding data processing, EU guidance exists to ensure data processed outside the EU is properly protected. Elected Technologies has stated that all data held within the Casework System is stored and processed electronically within Google's EU data centres in Belgium and London. The provider's contract with Google is with their EU entity and includes GDPR EU approved Model Contract Clauses suggesting that some of the data may also processed outside the EEA. The provider has a single third-party processor that is legally based outside the EU that they use for outbound transactional emails only, and their data processing with them is covered by a specific data processing agreement, the EU/US Privacy Shield and GDPR EU approved standard contract clauses (SCCs).

The OPCC's contract with Elected Technologies will include EU approved SCC's so as to provide adequate legal safeguards in relation to any data that is transferred outside the EEA, in compliance with DPA 2018 (see section on 'Context' – page 4). The parties will contract under the CCS G-Cloud framework and the OPCC will provide written instructions to Elected Technologies (who are a data processor under this arrangement) by the adoption of a data processing schedule

A copy of the providers NCSC Cloud principles is attached, along with a Data Processing Agreement that forms part of their Terms of Service (Appendix 1 of the ToS).


Caseworker.gov NCSC Cloud princip


Appendix 1 - Data Processing Agreeme

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The utilisation of a Casework System and the related processing of data is singularly in support of the legal responsibilities and duties of the PCC. As set out above, the role of the PCC is to be the voice of the people and hold the Chief Constable to account, effectively making the police answerable to the communities they serve. The PCC is responsible for the totality of policing and aims to cut crime and deliver an effective and efficient police service within Warwickshire. The PCC ensures community needs are met as effectively as possible, and improves local relationships through building confidence and restoring trust. The PCC works in partnership across a range of agencies at local and national level to ensure there is a unified approach to preventing and reducing crime.

Detailed information on the powers and responsibilities of the PCC is set out on the Home Office website, but in summary under the terms of the Police Reform and Social Responsibility Act 2011, the PCC for Warwickshire must:

- Secure an efficient and effective police for their area;
- Appoint the Chief Constable, hold them to account for running the force, and if necessary dismiss them;
- Set the police and crime objectives for their area through a police and crime plan;
- Set the force budget and determine the precept;

- Contribute to the national and international policing capabilities set out by the Home Secretary; and
- Bring together community safety and criminal justice partners, to make sure local priorities are joined up.

The benefits of processing data through the Casework System and the intended effect on individuals can be summarised as being the positive achievement of these responsibilities on their behalf in a way that ensures compliance with GDPR. Records will be stored in one location, from which data can be quickly and efficiently searched, retrieved, amended and deleted, as necessary.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The project to deliver the Casework System for the OPCC has consulted fully with all members of OPCC staff, as well as representatives from Warwickshire Legal Services. In addition, consultation with the Strategic Change Team and ICT Department of Warwickshire Police has been undertaken and was necessary as a result of the Force providing the ICT-related infrastructure, hardware, technical support and Information Security to the OPCC. As required under GDPR the ICT Department has undertaken due diligence of the Casework system, including a review of Elected Technologies' National Cyber Security Centre (NCSC) Cloud principles document. The outcome of the due diligence was a broad acceptance of the security of the system and its compliance with the requirements of GDPR, subject to any additional measures deemed necessary by the ICO as a result of the Schrems II case (yet to be determined)

Additionally, there has been liaison with Elected Technologies, provider of the casework system, who will act as a data processor in the processing of OPCC data. This has included a demonstration of the Casework system to all staff.

It is not considered necessary or proportionate to undertake consultation with the public of Warwickshire regarding the introduction of a Casework System for the OPCC. As highlighted previously, similar technology is in widespread use across the public and private sector and it is likely that any source of correspondence/contact with the OPCC will likely believe such a system is in already in use by the team.

That aside, it is not considered necessary or proportionate because from a holistic perspective, the total amount of correspondence/contacts received by the OPCC for Warwickshire (approx. 2,300 per year) and therefore the volume of data being processed, is very small in comparison to other organisations. Whilst this does not alter the legal responsibilities of the office under GDPR, nor reduce the potential impacts upon an individual if their data is misused or misplaced, it does position the overall risk of data processing by the OPCC as being low.

In addition, the vast majority of data to be processed through the Casework System is individually classified as fairly 'low risk' under GDPR. The OPCC does occasionally find itself processing Special Category and/or Criminal Offence data, but usually not in large volumes so as to be classified as 'high risk' by volume under GDPR.

In a small number of cases the OPCC may process data that might endanger the individual's physical health or safety in the event of a security breach, but does so in accordance with its GDPR-compliant 'Records Management Retention and Disposal Policy' and 'Retention Schedule'.

Furthermore, the OPCC is **not** engaged in the following high-risk data processing activities:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
- Systematic monitoring of a publicly accessible area on a large scale.
- Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (recitals 71 and 91).
- Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35(3)(a)).
- Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area" (Article 35(3)(c))15.
- Data processed on a large scale
- Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
- Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.
- When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91).

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The measures taken by the OPCC to ensure GDPR compliance and proportionality in the use of the Casework System are set out in the following documents:

Records Management and Retention Policy:  FINAL Records Management and R	Data Retention Schedule:  FINAL Retention Schedule 04.12.19.p
Record of Processing Activities:  Record of Processing Activity (I	Appropriate Policy Document:  Appropriate Policy document OPCC Jul
Full Privacy Notice:  Full Privacy Notice (Update 13.08.20).pc	
NCSC Cloud Principles  Caseworker.gov NCSC Cloud princip	Data Processing Agreement:  Appendix I - Data Processing Agreeme

In addition, a written contract (under the CCS G-Cloud framework) will exist with the provider of the Casework System that will set out clear instructions. A formal review of activity will take place every 12 months. OPCC Warwickshire will retain a right of audit of the system and will seek copies of the outcome of any independent audits completed by the provider.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)
The processing of data in the Cloud is not secure and data is compromised resulting in a data breach incident. Impact on individuals is potentially significant with the resulting financial and reputational implications for the OPCC. Furthermore, this will impact on the OPCC's ability to comply with data subjects' rights	Possible	Severe	High
The Caseworker system is not GDPR compliance e.g. records cannot be deleted	Possible	Significant	Medium
Elected Technologies do not meet their obligations under the SLA resulting in the system not being accessible to staff at least 99% of the time.	Possible	Minimal	Low
Staff do not use the case management system correctly	Possible	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** (Eliminated reduced accepted)	**Residual risk** (Low medium high)	**Measure approved** (Yes/no)
The processing of data in the Cloud is not secure and data is compromised resulting in a data breach incident. Impact on individuals is potentially significant with the resulting financial and reputational implications for the OPCC. Furthermore, this will impact on the OPCC's ability to comply with data subjects' rights	Due diligence has been undertaken and the ICT Dept has reviewed the NCSC document and concluded that the system meets required standards of security and compliance with the requirements of GDPR, subject to any additional measures deemed necessary by the ICO as a result of the Schrems II case (yet to be determined) Feedback received from other users of the Casework system. No security concerns have been raised WLS has undertaken a review of the ECJ recent decision to invalidate use of the EU-US Privacy Shield, provided some initial advice, and we now await ICO guidance on any additional necessary additional measures.	Reduced	Medium	Yes
The Caseworker system is not GDPR compliance e.g. records cannot be deleted	Demonstration of the Caseworker system has been provided to staff. Staff satisfied that the latest version of the Casework system has been designed in compliance with GDPR	Reduced	Low	Yes
Elected Technologies do not meet their obligations under the SLA resulting in the system not being accessible to staff at least 99% of the time.	Feedback from other users of the Casework system is that the system is reliable and that ET provide responsive support Contractual remedies should minimise risk	Reduced	Low	Yes

Staff do not use the case management system correctly leading to potential GDPR issues e.g. data held not being accurate	All staff have received a demo of the Casework system and will receive formal training on the use of the system (either directly from ET or from a colleague who has been trained by ET to train other staff members). A helpdesk facility is available from ET	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Neil Hewison, Chief Executive, OPCC for Warwickshire	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Neil Hewison, Chief Executive OPCC for Warwickshire	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Warwickshire Legal Services (Katherine Lamyman)	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: DPO advice has been sought throughout the process of undertaking the DPIA. Consultation has also taken place with the supplier, Force ICT colleagues and other users of the system allowing due diligence to be completed with a greater understanding of the system. The outcome of the due diligence was a broad acceptance of the security of the system and its compliance with the requirements of GDPR, subject to any additional measures deemed necessary by the ICO as a result of the Schrems II case. Initial risks have been minimised, as set out in Step 6, and any residual risks (which are not deemed to be high risk) will continue to be subject to review and additional measures introduced to further minimise risk, if deemed necessary.		
DPO advice accepted ~~or overruled~~ by:	Neil Hewison, Chief Executive, OPCC for Warwickshire	If overruled, you must explain your reasons
Comments: This DPIA in my view fully discharges the OPCC's responsibility to conduct such as assessment in relation to the new OPCC caseworker system. It is comprehensive. It details the consultation that has taken place, specifies how the system will deliver GDPR compliance with OPCC's processing of personal data and the steps that will be taken to minimise the residual risks associated with the implementation of the system.		
Consultation responses reviewed by:	Richard Long, Development and Policy Lead, OPCC for Warwickshire	If your decision departs from individuals' views, you must explain your reasons

Comments: Decision does not depart from views expressed during internal consultation. External consultation has not taken place.		
This DPIA will kept under review by:	Debbie Mullis, GDPR Lead, OPCC for Warwickshire	The DPO should also review ongoing compliance with DPIA