

Data Protection Impact Assessment.

Author	██████████
Owner	██████████
Date approved	07/10/2021
Current Version	V2.2
Review date	07/10/2021

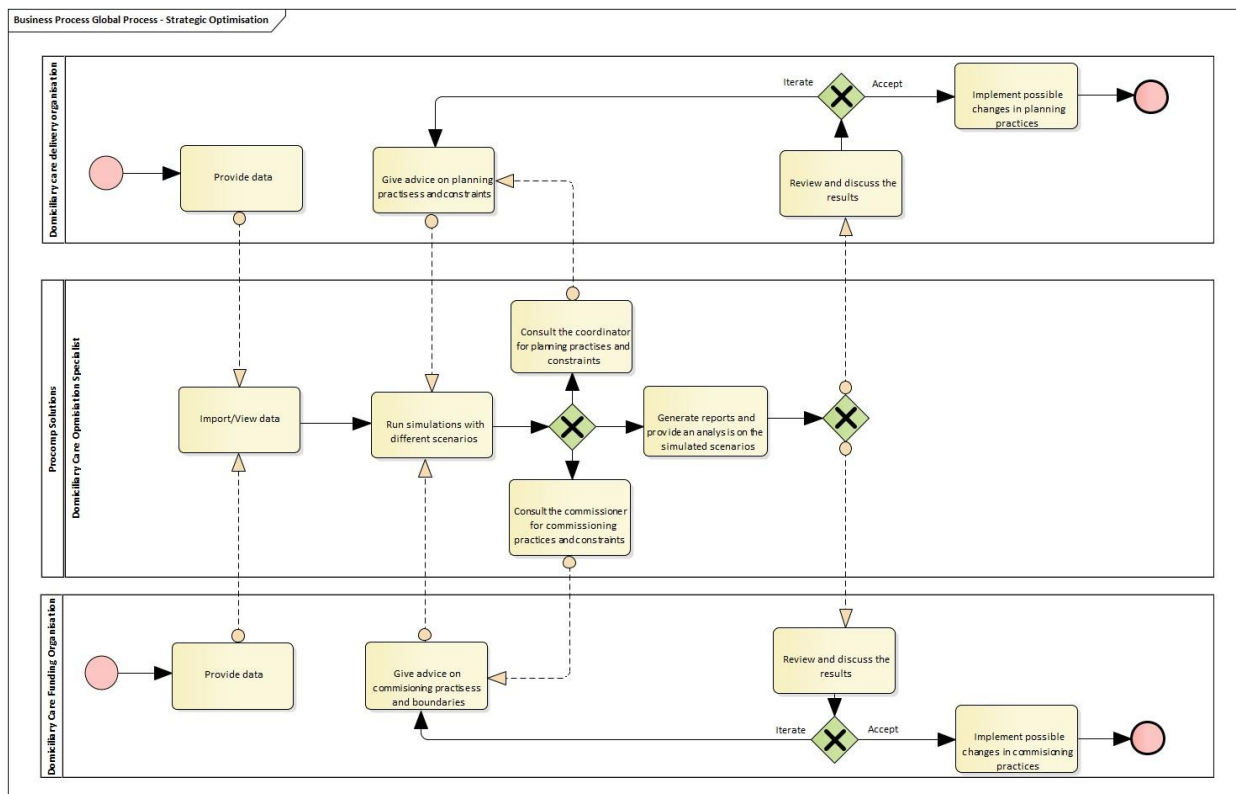
Version History

Version	Date	Author	Changes	Reviewer
1.0	08/09/2021	██████████	First version	
1.1	14/09/2021	██████████	Add info in Section 1	
1.2	15/09/2021	Procomp	Review	Procomp
2.0	17/09/2021	Procomp	Approved version	Procomp
2.1	05/10/2021	██████████	Minor amendments following NHS comments	Procomp
2.2	07/10/2021	██████████	Minor amendments following NHS comments	Procomp

Section 1: Background Information

Project Name:	R2 Domiciliary Care Strategic Optimisation
Organisation	Procomp Solutions Oy
Assessment Completed By	██████████
Job Title	████████████████████
Phone	██████████
E-mail	████████████████████
<p>Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required.</p> <p>It is widely recognised that there are significant pressures on the Domiciliary Care workforce (both in social and health care settings). Deep structural and systemic issues limit overall quality & efficiency and mean that changes are needed to the way Domiciliary Care is organised, commissioned and delivered. Despite the strong need for change, meaningful changes are not made because the logistical complexity makes it extremely difficult to know which changes will have the desired outcomes.</p> <p>Domiciliary Care is a logistics problem; the right person needs to be in the right place at the right time. Procomp's origins are in transport logistics planning and optimisation, and R2 Strategic Optimisation is a service which Procomp have adapted from the logistics domain to enable workable solutions to be found to structural and systemic issues in Domiciliary Care. Procomp have gained a wealth of experience improving the quality and productivity of domiciliary, having carried out over 60 Domiciliary Care Strategic Optimisation projects in Finland, representing 1/3 of the domiciliary Care workforce alternative scenarios, as well as projects in the Benelux countries.</p> <p>R2 Domiciliary Care Strategic Optimisation is a technology-enabled service where a snapshot of operational data is taken and Procomp's advanced Artificial-Intelligence-based planning tool (R2 Optimiser) is used to perform detailed modelling of alternative scenarios which would be difficult or impossible to test in the field through trial and error. These scenarios can be used to investigate the impact of any number of potential changes, for example:</p> <ul style="list-style-type: none">• Changes to care assessment and care planning practices• Changes to commissioning and brokerage practices• Changes to roles and shares of responsibility in integrated teams• Changes to work patterns• Outsourcing and insourcing of services• Changes to area structures and team sizes• Effect of taking certain equipment into use <p>The evidence provided by this detailed modelling enables informed decisions to be made regarding which changes to adopt and implement.</p> <p>The Strategic Optimisation process typically includes representatives from all stake holders so the anybody is able to put forward proposals and ensure that their needs are considered and has the benefit of making changes easier to take forward and adopt in live use.</p> <p>The objective of Strategic Optimisation is typically to improve productivity, quality of care, or worker satisfaction, and the outcome is typically an improvement in all these areas.</p> <p>Procomp consultants deliver analysis and reporting on the modelled scenarios, enabling the client to make informed decisions on which changes, or combination changes to adopt and in which sequence. Strategic Optimisation provides great value on its own, however, organisations may opt to gain further operational benefits by taking Procomp Solutions' R2 Operational Optimisation into use. Please note, that this DPIA refers only to the Strategic Optimisation Product. R2 Operational Optimisation is described in a separate DPIA.</p>	

Please find a high-level process for Strategic Optimisation below:



Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.

The Domiciliary Care Strategic Optimisation objectives are typically to:

- Provide understanding of the structural and systemic factors involved and how they affect Domiciliary Care service delivery and utilisation of the workforce
- Identify the structural and systemic changes which will have the desired outcomes on domiciliary care service quality and workforce utilisation
- Improve efficiency and utilisation of the care workforce by lowering mileage, gaps and the number of care workers needed
- Improved Quality metrics: Continuity and Planned vs Delivered service time
- Improve Carer Worker satisfaction by providing more stable, less fragmented work shifts with less rush and realistic time for travelling

What are the purposes of collecting the information within the system? For example, patient treatment, patient administration, research, audit, reporting, staff administration etc.

Strategic Optimisation requires a snapshot of operational data which is then used to model alternative scenarios in order to identify systemic and structural changes which will lead to improvements in Domiciliary Care service delivery and utilisation of the workforce. No actual service user visits are planned during the Strategic Optimisation project.

The purpose of collecting the information in the system is to enable modelling of alternative scenarios. The evidence provided by this detailed modelling enables informed decisions to be made regarding which changes to adopt and implement.

Data needed in Strategic Optimisation projects is usually collected from the Domiciliary Care commissioning authority and/or providers' existing ERP or patient management system. The organisation delivers the data (e.g. in a spreadsheet or txt file) using secured channels (secured email or secured file sharing). Data covering a minimum period of one week is required, typically representing a period in the past (so that actuals are also available)

Data is pseudonymised and includes:

- A unique identifier (e.g., GUID) for each service user -> the name of the client should be removed before sending the data to Procomp.
- An identifier representing the domiciliary care delivery organisation

- Postal code
- Earliest and latest permissible start time of visit
- Service time of visit (duration)
- Service requirements of the visit (type of care worker or special skill requirement for care worker to take care of visit)
- Actual visit start and end times (if actuals are available)

The data is stored in a folder on Procomp's network. Access to the folder is limited to users necessary to process data. The data is processed and modified to the format that R2 Optimisation software requires and is imported to the software's database. Data is not shared with anyone. Access to the data in R2 is limited to users necessary to process data.

All data received and produced during preprocessing (including database) is deleted after the project.

Please see the attached high-level data process 'Procomp R2 Strategic Optimisation project - Handling of data. '

What are the potential privacy impacts of this proposal - how will this change impact upon the data subject? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing.

The potential privacy impacts are limited because of the following

- The only actual client information that is required is the postcode (though in a small number of cases it may be possible to deduce other data, e.g. a request for a female carer is likely to mean a female client) where the visit should take place
- The organisation is asked to remove other data (e.g. customer names) before sending it to Procomp
- We do not need to know the age or gender of the client
- Scenario modelling is based on virtual care workers – no real care worker names or data needed
- Other requirements (e.g. care worker gender preferences, care worker skills) can be handled as parameters and settings
- No information is requested which is not already held

Provide details of any previous DPIA or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a DPIA may have been undertaken during the project implementation

This is the first DPIA.

Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change.

Whilst this project is introducing our strategic optimisation service to the UK, the service has been in existence for a number of years in Finland and other countries and has been well received with no concerns raised. It is a service used internally by organisations without any direct impact on patients/clients, so they have not been involved in the development of the service. The service was developed internally by Procomp but when the service is adopted the following stakeholders are involved.

Procomp: Consultant, Optimisation system specialist, Developer

Domiciliary Care Delivery Organisation: Manager, Co-ordinator (planner), Domiciliary Care worker

Commissioning Organisation: Manager, Commissioner

Section 2: The Data Involved

Patient Data type		Justifications
Information that identifies the individual and their personal characteristics	Name	No
	Address	No
	Postcode	Yes
	Dob	No
	Age	No
	Sex	No
	Gender	No
	Racial/ethnic origin	No
	Physical description	No
	NHS number	No
	Mobile/home phone no.	No
	Email address	No
Patient Data type		Justifications
Information relating to the individual's physical or mental health or condition		Yes
Information relating to the individual's sexual life		No
Information relating to the family of the individual and the individual's lifestyle and social circumstances		No
Information relating to any offences committed or alleged to be committed by the individual		No
Information relating to criminal proceedings, outcomes and sentences regarding the individual		No
Information which relates to the education and any professional training of the individual		No
Employment and career history		No
Information relating to the financial affairs of the individual		No
Information relating to the individual's religion or other beliefs		No
Information relating to the individual's membership of a trade union		No

Postcode information is needed for calculating accurate travel time between visits when modelling scenario.

None of the listed information is collected directly within the service application but we accept that analysis of the data can reveal some information about the patients/clients involved, e.g. post code can occasionally be disclosive, details of care worker skills and requests for particular characteristics of care workers can inform about care needs and gender etc. Within the context that the data are processed they are essentially anonymised but we accept that under GDPR a small amount of the data are actually pseudonymised and could lead to identification when combined with other publicly obtainable data.

Section 3: Assessment

	Question	Patient/Client data
Legal compliance - is it fair and lawful?	1. What is the legal basis for processing the information? <i>This should include which conditions for processing under the GDPR apply and how the common law duty of confidentiality will be met.</i>	To the extent that the data falls under GDPR the legal basis must be determined by our customers, the data controllers. Procomp is a data processor for this data. The legal basis will likely be the public interest (Article 6(1)(e) and 9(2)(h)) in respect of managing care delivery. Only a small amount of data will actually fall under the provisions of GDPR, the great majority will be anonymised data. The absence of direct identifiers and the secure context within which it is processed means that there is no breach of confidentiality, so the common law is not applicable.
	2. a - Is the processing of individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act? b - Have you identified the social need and aims of the initiative and are the planned actions a proportionate response to the social need?	The processing of data by this service will not interfere with the 'right to privacy' under Article 8 of the Human Rights Act as no individual will be identified. More efficient and effective care services are in the interests of society.
	3. It is important that individuals affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed?	This is the responsibility of our customers, but we have found that the majority already inform patients/clients that data will be used to improve services.
	4. If you are relying on consent to process personal data under the GDPR, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?	Consent is not required.
	5. Is a form of consent needed to satisfy common law confidentiality requirements? If not, why not?	Consent is not required as confidentiality is not impacted.

Purpose	6. Does the project involve the use of existing personal data for new purposes?	Only minimal personal data is involved i.e. where a Postcode relates to a single household but the analysis we provide is an improved method rather than a new purpose for using the data.
	7. Are potential new purposes likely to be identified as the scope of the project expands?	We are planning to offer an Operational Optimisation product in the UK (and which is already in use in other EEA countries), which will require more data, but a new DPIA will be completed for this.
Adequacy	8. Is the information you are using likely to be of good enough quality for the purposes it is used for?	We work with the customer to ensure that data is of sufficient quality, and this is not usually an issue.
Accurate and up to date	9. Are you able to amend information when necessary to ensure it is up to date?	Data can be amended where necessary, either in Procomp's systems or by importing fresh data from the customer's systems.
	10. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	This is the responsibility of our customers
Retention	11. What are the retention periods for the personal information and how will this be implemented?	Data is kept in Procomp's environment for the length of the project as determined by the contract with our customer. Please see the flow in section 1, Background / What are the purposes
	12. Are there any exceptional circumstances for retaining certain data for longer than the normal period?	No.
	13. How will information be fully anonymised or destroyed after it is no longer necessary?	After projects end: <ul style="list-style-type: none"> • Data from network drive is deleted • Customer specific R2 database(s) are deleted
Rights of the individual	14. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held?	Procomp cannot identify individuals so this must be actioned by our customers.

Appropriate technical and organisational measures	15. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?	Only a small number of staff can access data and only when necessary to fix issues. These staff have all undertaken or will shortly undertake online information governance training. A Learning Management System is used which provides the necessary audit capabilities.
	16. If you are using an electronic system to process the information, what security measures are in place?	All data is received from the client via our secure file share service (using SSL/TLS encryption protocols) is saved to Procomp's network folder. All work files (during conversion of data) are also saved to the same network folder and secured with AES 256-bit encryption. Converted data is then imported to customer specific R2 database for Strategic scenario optimisations. Access to folders and to the database is allowed only to a small number of staff. More detail of security can be found at https://www.sharefile.com/secure-file-sharing
	17. How will the information be provided, collated and used?	The customer will share data with Procomp via a secure file share service, for example Procomp's secure file share service. On Procomp's side, the data will be saved to our network drive, where data is converted to the format required by R2 Optimisation software. After conversion, the data is imported to the software from excel file and saved to a customer specific R2 database.
	18. What security measures will be used to transfer the identifiable information?	Procomp uses a secure file transfer service.
Transfers both internal and external including outside of the EEA	19. Will individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?	No disclosures will take place
	20. Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data?	No. All data is kept inside the European Economic Area.
Consultation	21. Who should you consult to identify the privacy risks and how will you do this? Identify both internal and external stakeholders.	We utilise a third-party security service which undertakes regular penetration testing. Our Info Security lead is required to undertake continuing professional development and we have consulted our UK based DPO.

	22. Following the consultation - what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc.	The only privacy risk identified has been the possibility of a Postcode relating to a single residence. This is rare and only a small number of staff have access to the data in limited circumstances, so the risk is minimal.
Guidance used	23. List any national guidance applicable to the initiative that is referred to.	NHS Confidentiality Code of Practice ICO guidance on an Anonymisation and data protection

Section 4: Risk Assessment

The following risks have been identified while conducting a risk assessment for the Strategic Analysis

Risk	Likelihood	Impact	Risk Score	Mitigation
Failure of critical system/function	1	3	3	Strategic Optimisation is not a real-time service. Backups are made at least every night, to a duplicate system. Restoring back up's is tested regularly.
Poor data quality invalidates analysis	1	3	3	In the Strategic Optimisation projects the data is usually imported with a .csv or .xls file. We perform data analysis to audit the quality of the data and review and cleanse it together with the customer.
Staff misusing access privileges	1	3	3	Accurate process for user rights definition and protection of data. <ul style="list-style-type: none"> The data in Strategic Optimisation projects pseudo anonymised which limits the potential for misuse Adequate guidance, limited user rights, employment contract is binding, NDA is signed All activity associated with our systems is logged and only a small number of senior staff may access these logs for forensic investigation. Maintain a register of which staff have access to data. Dependent upon their role, very few staff have these access permissions. Robust procedure for managing the exit of staff from roles or from the organisation, including consideration of how their IT and data access requirements may change
Data being sent to the wrong recipient	1	3	3	We are not using regular email system to transmit data. A secure file sharing system is used. A separate folder(s) is (are) generated in this system for each customer and only specified persons from the customer organisation have access to the folder(s).

[illegible]