NIPEC/20/12

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

# Data Protection Impact Assessment (DPIA) Policy and Procedure

## January 2021

Any request for the document in another format or language will be considered

Centre House
79 Chichester Street
BELFAST
BT1 4JE

Tel: 0300 300 0066

https://nipec.hscni.net

| | |
|---|---|
| **Developed by:** | Janet Hall |
| **Approved by / date:** | **BTM:** 12th January 2021<br>**Council:** 8th February 2021 |
| **Date of next Review:** | January 2024 |
| **Equality Screened by / date:** | Corporate Services Manager, February 2021 |

# CONTENTS

## 1. Introduction

NIPEC must ensure that any processing of personal information for which it is responsible complies with the General Data Protection Regulations (GDPR) and the Data Protection Act (DPA) 2018.

GDPR introduced new obligations which require public authorities to integrate data protection concerns into every aspect of their processing activities. This approach, 'data protection by design' (the consideration of data protection at the very onset of any project), and 'data protection by default' (only processing the data that is necessary to achieve a specific purpose), requires NIPEC to consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

Under Article 35 of the General Data Protection Regulation (GDPR), data controllers will be legally required to undertake Data Protection Impact Assessment (DPIA) prior to data processing which is *"likely to result in a high risk to the rights and freedoms of natural persons*".

This policy will provide officers with guidance on how to assess whether a DPIA is required, and subsequently how to undertake and document a DPIA.

Specifically, this document is designed to assist in the identification and assessment of risks to personal information, as well as to assist in the documentation of envisaged safeguards and control measures in proportion to the risks identified.

## 2. What is a Data Protection Impact Assessment?

A DPIA is a process or tool to help an organisation analyse, identify and minimise privacy risks when processing personal information in any project – essentially, it is a tool used:

- To identify whether a proposed project is likely to impact on the privacy of individuals affected, either positively or negatively;
- To check whether your project is likely to comply with the data protection principles;
- To make decisions about whether and how to adjust the proposal to manage any privacy risks and to maximise the benefits of protecting privacy;
- As a reference point for future action as the project or process changes.

A DPIA will assess the impact of data processing operations on the protection of personal information, ensure that the protection of personal data collected as part of projects and processes is considered at the appropriate times and stages, and assess the likelihood and severity of risks for the rights and freedoms of individuals resulting from this operation. A DPIA is not required in all circumstances but is relevant for new projects or proposals and when planning to make changes to an existing system.

The term 'project' is used in this policy in its widest possible sense to refer to any activity or function where the collection or processing of personal data is being considered. It could refer to the development of a new system, database, programme or application, a new policy or initiative, an enhancement to or review of an existing process or a new way of working.

This policy will provide officers with guidance on how to assess whether a DPIA is required, and subsequently how to undertake and document a DPIA.

Specifically, this policy is designed to assist in the identification and assessment of risks to personal information, as well as to assist in the documentation of envisaged safeguards and control measures in proportion to the risks identified. As such, this policy shall also be considered integral to NIPEC's wider risk management process.

## 3. Benefits

A DPIA will assist NIPEC in a structured way to identify, categorise and mitigate privacy risks when processing personal information. Designing projects, or developing policies, with privacy in mind at the outset can lead to benefits which include:

- Identifying potential problems at an early stage, when addressing them will often be simpler and less costly;
- Increased staff awareness of privacy and data protection;
- Meeting our legal obligations and reducing the likelihood of a breach of data protection legislation;
- Ensuring our actions are less privacy intrusive and unlikely to have a negative impact on data subjects;
- Providing reassurance to individuals that NIPEC has followed best practice when using their personal data;
- Improved transparency, making it easier for individuals to understand how and why we are using their information;
- Building trust with people who use our services;
- Better information management practices.

## 4. When is a Data Protection Impact Assessment required?

Consideration of a DPIA is a mandatory requirement for any project, large or small, that:

- Involves collection of personal information – that is, information about living people, who can be identified;
- Involves information that may be used to identify, profile or target individuals;
- May result in surveillance of individuals or intrusions into their personal space or bodily privacy; or
- May otherwise affect whether people's reasonable expectations of privacy are met.

A DPIA must be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of individuals (taking into account of both the likelihood and severity of any potential harm). If in doubt, a DPIA should be carried out.

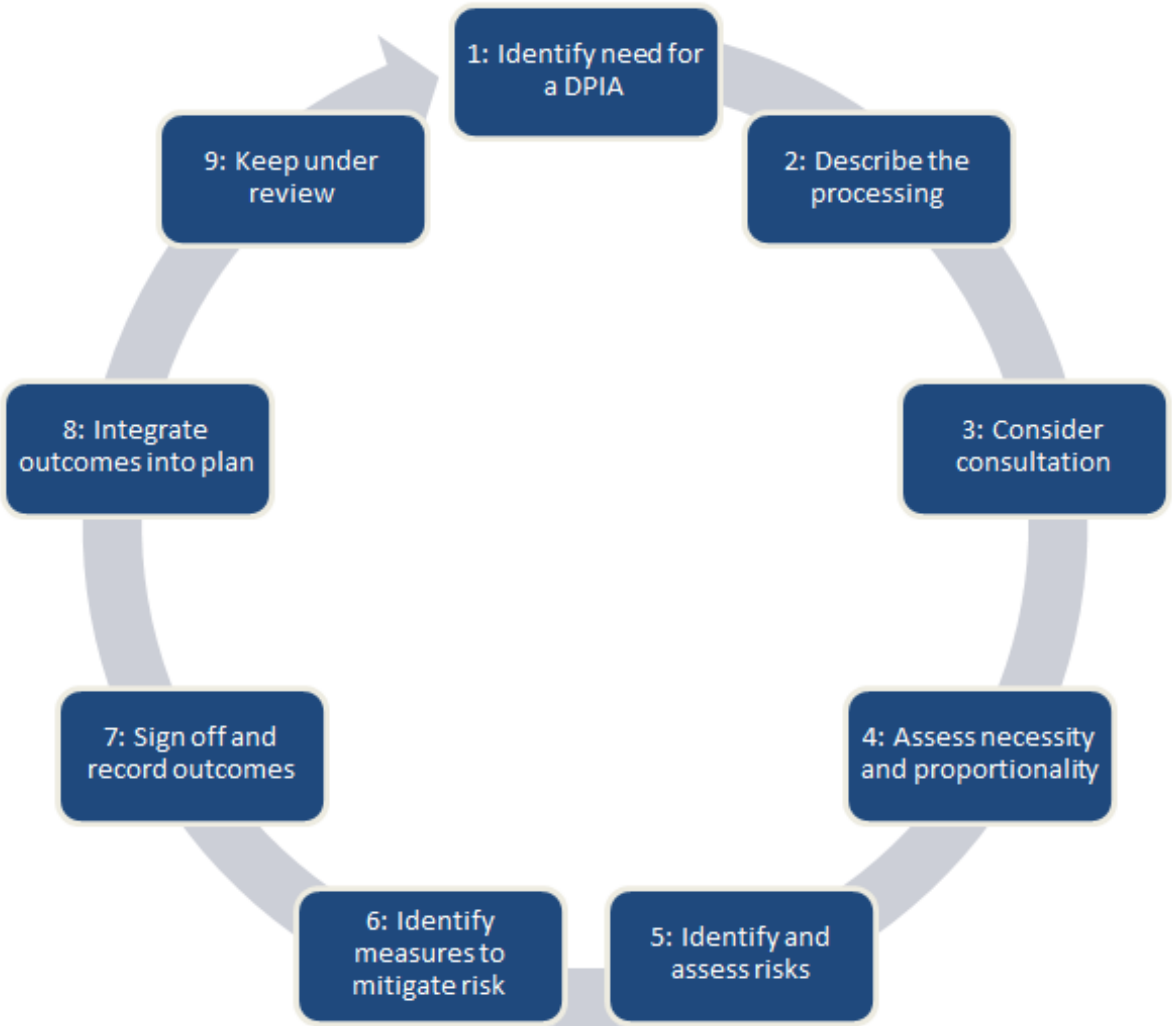
With existing systems or processes the following criteria should also be considered:

- significant changes that expand beyond the original purpose(s);
- new types of information to be processed are introduced;
- unexpected personal data breach with significant impact, the occurrence of which had not been previously identified;
- a periodic or defined review is triggered;
- in response to significant internal or external stakeholder feedback or inquiry;
- if there are technological-related changes that may have data protection implications.

## 5. How to undertake a Data Protection Impact Assessment

Consideration of the need for a DPIA should begin early in the life of a project before you begin processing, and run alongside the planning and development process. It includes the following steps:

- Screening exercise
- Full DPIA:
  - Step 1: identify the need for a DPIA
  - Step 2: describe the processing
  - Step 3: consultation process
  - Step 4: assess necessity and proportionality
  - Step 5: identify and asses risks
  - Step 6: identify measures to reduce risks
  - Step 7: approval process
  - Step 8: implementation (integrate outcomes into project plan)




*(taken from GDPR Data Protection Impact Assessments (DPIAs) ICO, March 2018)*

Depending on the nature and scale of the project, a number of people should be involved in considering and undertaking a DPIA. These should include (but not be limited to) the project lead/senior manager/Information Asset Owner (IAO), project team/steering group, website governance team etc.

## 6. Screening Exercise (to decide if a full DPIA is needed)

At the start of any project involving the processing of personal data, the project lead/IAO will be responsible for considering the requirement for a DPIA. The screening exercise (see Appendix 1) is designed to assist with this process and enable an initial analysis of the project in question at a 'high level' and help decide whether or not it will be necessary to conduct a full DPIA.

The project lead/IAO may decide after completing the screening exercise that the project does not require a DPIA because, for example, the project does not involve personal data, or the information used will be uncontroversial or the privacy risk is negligible. This should be formally recorded as the outcome of the screening exercise.

The details collected through the screening exercise should be retained as part of the project records and will provide transparency regarding the processes undertaken. If issues around privacy considerations arise at a later stage, information within the screening exercise can be used to demonstrate accountability.

If it is decided a full DPIA is required, the information recorded as part of the screening exercise will form the basis of a full DPIA. The DPIA template report (see Appendix 2) allows for the recording of information in a standardised format and follows a step by step process.

## 7. Full Data Protection Impact Assessment (DPIA)

Following the step by step process outlined in section 5, and using information gathered from the screening exercise, the project lead/IAO should record their decisions within the full DPIA report (Appendix 2).

The completed report is the formal record of the DPIA process and should clearly document all the steps of the DPIA, contain or reference other relevant information, e.g. consultation records, and should be held alongside any business case or other project documentation, such as the PID.

Keeping a formal record will assure the public, NIPEC's Council and senior team, the ICO and other stakeholders that the project has been thoroughly assessed for risks. Once the report has been signed off, the project lead/IAO must ensure that the details of the assessment are entered in NIPEC's Information Asset Register (IAR) overseen by NIPEC's Head of Corporate Services (HoCS). The IAR is an inventory of information assets and their systems, including personal data held.

If, as a result of the new process being implemented, there will be a requirement to share personal data with another public body or organisation, the project lead/IAO, in discussion with the HCS, must ensure that suitable arrangements are in place in the form of a robust contract or data access agreement.

## 8. Responsibilities

- **NIPEC Council** has overall responsibility for risk management and this includes management of information and ensuring compliance in all areas of information governance;
- The **Chief Executive** is accountable to Council for the delivery of this policy;
- The **Data Protection Officer** (DPO) will advise on the production of screening and full DPIAs ;
- **All NIPEC Staff,** whether permanent, temporary, bank or agency workers, have a responsibility to ensure that they are aware of the requirements to protect personal information held by NIPEC. They are expected to familiarise themselves and adhere to this policy and relevant legislation, report any incidents in connection with this policy and take required mitigating action to ensure that incidents do not recur.

## 9. Non-Compliance

Compliance with this policy and any associated procedures will be monitored regularly and reports considered by the appropriate management. A failure to adhere to this policy and any associated procedures may result in disciplinary action.

## 10. Equality Statement

This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998.

The screening has identified specific equality impacts for … *[specify the groupings]* and outlines the way these will be addressed

**or**

No significant equality implications have been identified therefore the policy will not be subject to an equality impact assessment.

The equality screening has been published and can be accessed here http://www.hscbusiness.hscni.net/services/2166.htm.

## 11. Review

This policy is based on a regional HSC approach and will be monitored and reviewed in January 2024, or sooner, if a revised HSC policy is issued.

**Appendix 1**

NIPEC

# DATA PROTECTION IMPACT ASSESSMENT (DPIA) SCREENING EXERCISE TEMPLATE

| **PROJECT NAME:** | |
|---|---|

## 1. PROJECT SUMMARY

*Briefly describe your project, plan or proposal. Set out its purpose and any projected benefits.*

## 2. STAKEHOLDERS

*Identify the main stakeholders or bodies involved and their role in the project.*

## 3. BRIEF DESCRIPTION OF INFORMATION INVOLVED

| 4. PRIVACY ASSESSMENT | | | |
|---|---|---|---|
| *Use this checklist to assess the project for privacy risks. The questions below will help you consider whether a DPIA is necessary. Answering 'Yes' to any of the questions is an indication that a DPIA would be a useful exercise.* | | | |
| **Does the project involve any of the following?** | **Yes** | **No** | **If yes, explain your response** |
| **Information management** | | | |
| A change to an existing policy, process or system that involves personal information (for example, new legislation or policy that makes it compulsory to collect or disclose information). | ☐ | ☐ | |
| A change in location of a business area or branch (for example, plans to centralise a service or an office move). | ☐ | ☐ | |
| Any practice or activity that is listed on a risk register (for example, activities listed on your business area's risk register or health and safety register). | ☐ | ☐ | |
| **Collection** | | | |
| Collecting new information about an individual (for example, gathering information about individuals' participation in a new project). | ☐ | ☐ | |
| A new way of gathering personal information (for example, collecting information online rather than on paper forms). | ☐ | ☐ | |
| **Storage, security and retention** | | | |
| A change in the way personal information is stored or secured (for example, cloud storage). | ☐ | ☐ | |

| | | | |
|---|---|---|---|
| A change to how sensitive personal information is managed (for example, moving health records to a new database). | ☐ | ☐ | |
| Transferring personal information offshore (for example, using a cloud based application to store data). | ☐ | ☐ | |
| A decision to retain personal information for longer than previously kept (for example, keeping information for 10 years when you previously only held it for 7). | ☐ | ☐ | |
| **Use or disclosure** | | | |
| Using information classed as ‘sensitive personal data’ (for example, information about an individual’s health). | ☐ | ☐ | |
| Using personal data already held for a new purpose (for example, to monitor trends of a new infection). | ☐ | ☐ | |
| Disclosing information to a third party (for example, following a request from another organisation to provide information for a particular purpose). | ☐ | ☐ | |
| Sharing or matching personal information held in different datasets or by different organisations (for example, combining data with other information held on systems or sharing information to enable organisations to provide services jointly). | ☐ | ☐ | |

| | | | |
|---|---|---|---|
| **Individuals' access to their information** | | | |
| A change in policy that results in people having less access to information that you hold about them (for example, archiving documents after 6 months into a facility from which they cannot be easily retrieved). | ☐ | ☐ | |
| **Identifying individuals** | | | |
| Establishing a new way of identifying individuals (for example, a unique identifier, a biometric or online identity system). | ☐ | ☐ | |
| **New intrusions on individuals' property, person or activities** | | | |
| Introducing a new system for searching individuals' property, persons or premises (for example, adopting a new policy of searching data on mobile phones that have been returned for upgrading). | ☐ | ☐ | |
| Surveillance, tracking or monitoring of movements, behaviour or communications (for example, installing a new CCTV system or monitoring a member of staff's email account). | ☐ | ☐ | |
| Changes to premises impacting on private spaces where clients/staff may discuss personal data (for example, relocating a branch where sensitive personal data is processed). | ☐ | ☐ | |
| New regulatory requirements that could lead to compliance action against individuals on the basis of information about them (for example, adding a new medical condition to the requirements of a licence). | ☐ | ☐ | |

| | | | |
|---|---|---|---|
| Other privacy intrusions such as body searches, or intrusion into physical space. | ☐ | ☐ | |

| **Additional Comments/Notes** |
|---|
| |

| **5. INITIAL RISK ASSESSMENT** |
|---|
| If you answered 'Yes' to any of the questions in section 4, use the table below to give a rating - either Low (L), Medium (M), or High (H) – to each of the aspects of the project set out in the first column. If you answered 'No' to all the questions in section 4, move on to section 6. |

| **Aspect of the Project** | **Rating (L, M or H)** | |
|---|---|---|
| Level of personal data handling | L – Minimal personal information will be handled | ☐ |
| | M – A moderate amount of personal information (or information that could become personal information) will be handled | ☐ |
| | H – A significant amount of personal information (or information that could become personal information) will be handled | ☐ |
| Sensitivity of information | L – The information is not sensitive | ☐ |
| | M – The information may be considered to be, or may become, sensitive | ☐ |
| | H – The information is highly sensitive | ☐ |
| Significance of the changes | L – Only minor change to existing functions/activities | ☐ |
| | M – Substantial change to existing functions/activities; or a new initiative | ☐ |
| | H – Major overhaul of existing functions/activities; or a new initiative that's significantly different | ☐ |

| | | |
|---|---|---|
| Interaction with third parties | L – No interaction with other agencies | ☐ |
| | M – Interaction with one or two other agencies | ☐ |
| | H – Extensive cross-agency (government) interaction or cross-sectional (non-government and government) interaction | ☐ |
| Public impact | L – Minimal impact on the organisation and individuals | ☐ |
| | M – Some impact on individuals is likely due to changes to the handling of personal information; or the changes may raise public concern | ☐ |
| | H – High impact on individuals and the wider public; concerns over aspects of project or negative media interest is likely | ☐ |

| **6. SUMMARY OF PRIVACY IMPACT** | |
|---|---|
| **The privacy impact for this project has been assessed as:** | |
| **Low** – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated. | ☐ |
| **Medium * **** – Some personal information is involved, and several low to medium risks have been identified | ☐ |
| **High * **** – Sensitive personal information is involved, and several medium to high risks have been identified | ☐ |
| **Reduced risk –** The project will lessen existing privacy risks | ☐ |
| **Inadequate information** – More information and analysis is needed to fully assess the privacy impact of the project. | ☐ |
| **Briefly summarise reasons for the rating given** | |
| | |

* Refer to Section 5 (Special Category Data) in the DPIA Guidance when determining level of privacy impact.

** If you have assessed the privacy impact as high or medium, a DPIA must be carried out.

| **7. RECOMMENDATION** | |
|---|---|
| A full data protection impact assessment **is** required | ☐ |
| A full data protection impact assessment **is not** required | ☐ |
| **Reasons** | |
| | |
| **8. SIGN OFF** | |
| **Project Manager** | |
| Name: | Date: |
| Signed: | |
| **Senior Responsible Owner / Information Asset Owner** | |
| Name: | Date: |
| Signed: | |

**Appendix 2**

NIPEC

# DATA PROTECTION IMPACT ASSESSMENT (DPIA) REPORT TEMPLATE

| **DPIA Ref Number** *(HCS / CSM to provide)* | |
|---|---|
| | |
| **Project Name** | |
| | |
| **Information Asset Owner** | **Project Manager** |
| | |

**Note: Please delete all guidance notes in italics from your final report**

| **Step 1: Identify the need for a DPIA** |
|---|
| *Give a short overview of the project. You will have to provide more detail in sections below so it can be kept very brief.* |

| **Purpose** |
| --- |
| *Describe the project and what it is meant to achieve. It may be helpful to refer to other documents, such as a project proposal. (Information contained in the screening exercise a helpful starting point).* |
| **Need for a DPIA** |
| *Describe how the project will impact on privacy and why a DPIA was undertaken.*<br>*Identify if there are any limitations to the DPIA. For example, no arrangement in place to cover the use of personal information by third party.* |
| **Lawful Basis for Processing** |
| *In this section, set out your lawful basis for processing.* |

| **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?* |
| **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?* |
| **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)?* |

| **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?* |
| **Step 3: Consultation process** |
| *Set out your key stakeholders and their role in the project. This information may have been gathered for the screening exercise.* |
| **Consultation** |
| *Explain how you consulted with stakeholders and the extent of any consultation.* |

| **Step 4: Assess necessity and proportionality** |
| --- |
| *Describe compliance and proportionality measures. 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 transfers, including international transfers?* |

| Step 5: Identify and assess risks | | | |
|---|---|---|---|
| **Risk**<br>*Describe source of risk and nature of potential impact on individuals.*<br>*Include associated compliance and corporate risks as necessary.* | **Likelihood of harm**<br>*Almost certain, likely, possible, unlikely or rare* | **Impact (consequence) of harm**<br>*Insignificant, minor, moderate, major or catastrophic* | **Overall risk**<br>*Low, medium, high or extreme* |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| **Step 6 Identify measures to reduce risk** | | | | |
|---|---|---|---|---|
| *Explain how you could address each risk identified in Step 5. Some risks might be eliminated altogether and others might be reduced. For others, you may be required to accept some level of risk. Evaluate the likely costs and benefits of each approach. Think about available resources, and the need to deliver a project which is still effective.* | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk**<br>*Eliminated, reduced or accepted* | **Residual risk**<br>*Low, medium, high or extreme* | **Measure approved**<br>*Yes / No* |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| **STEP 7 Approval Process** | | |
|---|---|---|
| *Ensure privacy solutions are approved at an appropriately senior level. In general, the DPIA will be signed off by the responsible Information Asset Owner. For larger scale projects, the Senior Information Risk Owner will be required to approve solutions and sign off the process. In this section, you should summarise the steps taken to reduce risks to privacy and record decisions taken to eliminate, mitigate or accept the identified risks.* | | |
| **Item** | **Name/date** | **Notes** |
| Measures approved by: | | *Integrate actions back into project plan, with date and responsibility for completion (see step 8)* |
| Residual risks approved by: | | *If accepting any residual high risk, ICO must be consulted before going ahead. Advice of DPO must be sought first.* |
| DPO/Information Governance advice provided: | | *DPO/Information Governance to advise on compliance* |

| **Step 8 Implementation** | | |
|---|---|---|
| *What actions need to be taken forward as a result of the DPIA? Who is responsible for integrating DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved and what is the timescale? Who is responsible for any privacy concerns that may arise in the future?* | | |
| **Action to be taken** | **Date for Completion** | **Responsible Owner** |
| | | |
| | | |
| | | |
| | | |

| Contact point for future privacy concerns | |
|---|---|
| | |
| **SIGN OFF** | |
| | |
| **Senior Responsible Owner/Information Asset Owner** | |
| **Name:** | **Date:** |
| **Signed:** | |
| **Project Manager** | |
| **Name:** | **Date:** |
| **Signed:** | |
| **Chief Executive** | |
| **Name:** | **Date:** |
| **Signed:** | |