POLICY

Data Protection Impact Assessments

Policy Owner	Information Compliance Manager
Policy Holder	Compliance Officer
Author	Compliance Team

Policy No.	178

Approved by

Legal Services	N/A
Policy Owner	05.12.18
JJNCC	04.12.18

Note: *By signing the above you are authorising the policy for publication and are accepting responsibility for the policy on behalf of the Chief Constables.*

Publication Date	05.12.18
Review Date	05.12.21
APP Checked	November 2018
College of Policing Code of Ethics Checked	November 2018

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

Legislation specific to the subject of this policy document

Section	***Act (title and year)***
	General Data Protection Regualtion (GDPR) and Data Protection Act 2018
	Freedom of Information Act 2000
	Human Rights Act 1998
	Common law duty of confidentiality
	Equality Act 2010
	Computer Misuse Act 1990
	Protection of Freedoms Act 2012

Other legislation which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
Health and Safety at Work etc Act 1974 and associated Regulations
General Data Protection Regulation and Data Protection Act 2018
Freedom Of Information Act 2000
Common law duty of confidentiality
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Criminal Procedure and Investigations Act 1996 (CPIA)
Protection of Freedoms Act 2012
Regulation of Investigatory Powers Act 2000 (RIPA)

Other Related Documents

- Information Security Policy
- Records Management Policy
- Data Protection Policy

- Freedom of Information Policy
- Information Sharing Policy
- Information Risk Management Policy
- Information Asset Owners Policy
- Force Risk Appetite Statement
- Data Quality Policy
- DBS & CLPD Policy
- Information Audit and Monitoring Procedure
- Information Management Training Procedure

1. Policy Aim

1.1 This policy sits under the Information Management Policy.

1.2 This policy sets out how Norfolk and Suffolk Constabularies will manage Data Protection Impact Assessments (DPIA) in respect of any new policies, projects, initiatives or Information Sharing Agreements (ISA) that are to be formally approved.

1.3 The policy will explain the principles which form the basis for a DPIA and will set out the basic steps which both Constabularies should carry out during the assessment process.

1.4 This policy has been introduced to reflect the publication by the Information Commissioner's Office (ICO) of the guidelines relating to 'The Accountability and Governance: Data Protection Impact Assessments (DPIAs)'.

2. Applicability

2.1 Adherence to this policy should be observed by all Norfolk and Suffolk personnel.

3. What is a Data Protection Impact Assessment (DPIA)?

3.1 A DPIA is a flexible process, which will enable both Norfolk and Suffolk Constabularies to systematically and accurately identify and minimise the privacy risks of new policies, initiatives and projects while allowing the aims of the project to be met whenever possible.

3.2 An effective DPIA will be used throughout the development and implementation of a ISA / project, alongside existing project management processes.

3.3 A DPIA can be carried out for any ISA / project which involves the use of personal data, or to any other activity which may have an impact on the privacy of individuals. DPIAs are employed for new projects as this allows

a greater scope for influencing how the project will be applied but should also be considered for revisions of existing projects.

3.4 The GDPR states a DPIA must be conducted if the following apply:

- Use of systematic and extensive profiling with significant effects;
- Processing of special category or criminal offence data on a large scale; or
- Systematically monitoring publicly accessible places on a large scale.

3.5 The ICO also requires DPIAs to be completed if the following apply:

- Use of new technologies;
- Use of profiling or special category data to decide on access to services;
- Profiling individuals on a large scale;
- Processing biometric data;
- Processing genetic data;
- Matching data or combining datasets from different sources;
- Collecting personal data from a source other than the individual without providing them with a privacy notice;
- Tracking individuals' location or behaviour;
- Profiling children or targeting marketing or online services at them; or
- Processing data that might endanger the individual's physical health or safety in the event of a security breach.

3.6 Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.

3.7 The risks may be to the individuals affected (for instance, in terms of the potential for damage or distress) but will also include corporate risks such as any financial or reputational damage as a result of a data breach.

3.8 A DPIA will help to ensure potential problems are identified at an early stage and benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.

4. Why undertake a Data Protection Impact Assessment?

4.1 Conducting an effective DPIA should benefit the organisations by:

- Reassuring individuals who are subject to the processing of personal data, that the Constabularies are following best practice.
- Improving transparency and increasing public confidence in the way in which the Constabularies collect and use personal data.
- Allowing the Constabularies to consider if any improvements are required to the way that personal information is managed. This should consequently reduce the likelihood of the organisations failing to meet their legal obligations under the Data Protection Act (DPA) 2018 and various related legislation.
- Identifying potential risks early on in the project and thereby reducing costs associated with rectifying the issue at a later stage where the necessary changes are problematic to implement.
- Raising awareness of privacy and data protection issues within the organisations and ensure that all relevant staff involved in a project consider privacy issues at an early stage.

5. When should a Data Protection Impact Assessment be undertaken?

5.1 A DPIA must be completed before the Constabularies begin any type of processing which is "likely to result in a high risk[1]" i.e. factors that point to the potential for widespread or serious impact on individuals. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project or where significant changes are being made to an existing process/database involving the use of personal data.

5.2 If the Constabularies are introducing a new policy/ project/ initiative/ ISA or ICT system or are making significant changes to a process/ database etc. that has implications for the use of personal information, a DPIA should be considered.

5.3 A DPIA should start in the initial stages of a project, e.g. at project initiation phase or its equivalent or the business case stage. When it is apparent that a project will have some level of impact on privacy, the Constabularies should start to consider how these issues will be addressed. DPIAs are more likely to be of use when implemented in the early life of a project when it is possible to have a greater impact on the development of the task.

5.4 Starting a DPIA in the early stages of a project will help the Constabularies to understand any potential impact on privacy and what steps will need to be taken in order to identify and minimise the associated risks. This in turn will direct what resource levels should be dedicated to the assessment.

[1] Please see Appendix B for definition of High Risk processing.

5.5 The process should be comparable in size to the nature of the project. Small projects with comparatively low impact will require a less formal assessment.

6. Who should conduct a Data Protection Impact Assessment?

6.1 The Compliance Team will help to complete the DPIA, working closely with the policy, project or initiative manager.

6.2 An effective DPIA will involve various people in the organisations who will be able to identify different privacy risks and solutions, e.g. Information Security, Records Management and Data Protection. The policy, project or initiative manager will be responsible for ensuring that the identified risks are integrated into the project plan.

6.3 Please notify the Compliance Officer promptly of all new projects proposed to ensure appropriate advice and guidance is offered from the outset. As a data protection practitioner, the role is well-placed to assist with the identification of privacy risks, able to offer ongoing support during the project and complete the DPIA.

6.4 For large-scale projects with a higher level of risk, it is appropriate for the Senior Information Risk Owner (SIRO) to approve/ sign-off the DPIA and any associated risks. For smaller projects, it will be appropriate for the project manager to accept the privacy risks. If the SIRO decides to accept the high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, consultation will need to take place with the ICO before any processing can go ahead. Please contact the Compliance Officer to facilitate these referrals.

7. Data Protection Impact Assessments in Practice

7.1 A DPIA will aim to incorporate the following processes:

- Identify the need for a DPIA;
- Describe the processing;
- Consultation process;
- Assess necessity and proportionality;
- Identify and assess risks;
- Identify measures to reduce risk;
- Sign off and record outcomes;
- Integrate outcomes into project plan; and
- Keep DPIA under review

Identify the need for a DPIA

7.2 The first step is to identify the need for a DPIA, which the Compliance Team can assist with by providing a checklist to assess the need. If it is a major project which involves the use of personal data it is good practice to carry out a DPIA. Otherwise, you need to check whether the processing is on the list of types of processing that automatically require a DPIA. If this is not the case, screening of other factors need to be completed which may indicate that the type of processing is high risk.

7.3 If after the screening exercise it is decided that a DPIA is not needed, the decision and reasons why need to be documented including the advice sought from the Compliance Team and/or Data Protection Officer (DPO). This does not have to be an onerous paperwork exercise – as long as it helps demonstrate that that consideration has been made for a DPIA and complied with any obligations of the DPA.

7.4 Not all projects will need the same level of DPIA. The impact on privacy is larger when the data is sensitive or when its use is more intrusive. Most projects will benefit however from a methodical analysis of how personal data is used and a compliance check against the Data Protection Act 2018.

7.5 At this early stage in the process, the Constabularies should be able to establish the project objectives and desired outcomes. Ensure that the overall aims of the project are defined and explained in order that any privacy concerns can begin to be addressed.

7.6 Gaining support from senior management and discussing privacy issues with both internal and external stakeholders at the onset of the project will ensure the DPIA is effective.

Describe the processing

7.7 Understanding the processing involved in a project is crucial to supporting a proper assessment of privacy risks. The DPIA process should describe the nature, scope, context and purposes of the processing.

7.8 The **nature of the processing** is what the Constabularies plan to do with the personal data. For example, this should include:

- How data is collected
- How data is stored
- How data is used
- Who has access to the data
- Who is the data shared with
- Are any Processors being used?
- Retention periods

- Security measures
- Whether it is a new technology and/ or a novel type of processing
- Screening criteria that was flagged as high risk

7.9 The **scope of processing** is what the processing covers, for example this should include:

- The nature of the personal data
- The volume and variety of the personal data
- The sensitivity of the personal data
- The extent and frequency of the processing
- The duration of the processing
- The number of data subjects involved
- The geographical area covered

7.10 The **context of the processing** is the wider picture, including internal and external factors which might affect expectations or impact. For example, this may include:

- The source of the data
- The nature of relationship with individuals
- The extent to which individuals have control over their data
- The extent to which individuals are likely to expect the processing
- Whether they include children or other vulnerable people
- Any previous experience of this type of processing
- Any relevant advances in technology or security
- Any current issues of public concern
- Whether you comply with relevant legislation
- Whether you have considered and complied with relevant codes of practice.

7.11 The purpose of the processing is the reason why the Constabularies want to process the personal data. This should include:

- Lawful basis for processing
- The intended outcome for individuals
- The expected benefits for the Constabularies or for society as a whole

7.12 An incomplete understanding of how information is used can be a significant risk, e.g. data may be used unlawfully or disclosed inappropriately.

7.13 Describing how the information flows can assist in identifying privacy risks or any unforeseen uses of the data. Future data sharing opportunities can be highlighted along with other potential uses for the information.

7.14 Existing information audits and the Information Asset Register can be referred to in order to understand how personal data might be used.

Consultation Process

7.15 Consultation is an important part of a DPIA and should be undertaken with both internal and external stakeholders, throughout the DPIA process. Consultation allows people to highlight privacy risks and solutions based on their own area of interest or expertise.

7.16 Internal consultation will usually be with a range of internal stakeholders such as the project management team, information management, ICT, procurement and senior management to ensure that all relevant views are taken into account. A full range of stakeholders is easier to establish if some scoping work has already been carried out to identify the processing.

7.17 External consultation will mean seeking the views of the people affected by the project. Depending on the nature of the project, this may be members of the public, partnership working arrangements, interest groups, Independent Advisory Groups or Constabulary personnel outside of the range of the internal stakeholders listed above.

7.18 The terms of the consultation should be clear about which aspects of the project are open to change and which are less so. It may be more effective to consult on just one aspect of the project or several targeted aspects. Effective consultations should follow the following principles:

- Timely – at the right stage and allow enough time for responses
- Clear and proportionate – in scope and focused
- Reach and representative – ensure those likely to be affected have a voice
- Ask objective questions and present realistic options
- Feedback – ensure those participating receive feedback at the end of the process

Assess necessity and proportionality

7.19 To assess necessity and proportionality the following should be considered:

- Do the plans help to achieve the purpose of the project?

- Is there any other reasonable way to achieve the same result?

7.20 This section should also include how data protection compliance is ensured; this is a good way to measure the necessity and proportionality. In particular, the relevant details should be included:

- Lawful basis for processing
- How function creep is prevented
- How data quality is ensured
- How data minimisation is ensured
- How privacy information is provided to individuals
- How individuals' rights are implemented and supported
- Measures to ensure processors comply
- Safeguards for international transfers

Identify and assess risks

7.21 The DPIA process is a form of risk management. When conducting a DPIA, the Constabularies must consider how the project will affect an individual's privacy. Privacy risks usually have associated compliance risks and risks to the organisations. As well as establishing the risks to the individual, also assess the corporate risks, including regulatory action, reputational damage, and loss of public confidence and trust.

7.22 Consideration must be given to the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular, whether processing could contribute to:

- Inability to exercise rights
- Inability to access services or opportunities
- Loss of control over the use of personal data
- Discrimination
- Identity theft or fraud
- Financial loss
- Reputational damage
- Physical harm
- Loss of confidentiality
- Re-identification or pseudonymised data
- Any other significant economic or social disadvantage

7.23 Security risks should be objectively assessed, including sources of risk and the potential impact of different types of breaches (i.e. dishonest access to, alterations to or loss of personal data).

7.24 Please also refer to the Equality Impact Assessment policy to ensure that personal information is managed in such a way that complies with the Equality Act 2010 and assists in identifying any potential negative disproportionate impact on people or groups of people, specifically those identified as having a protected characteristic as defined by the Equality Act 2010.

Identify measures to reduce risk

7.25 The objective of the DPIA is not to entirely remove the impact on privacy but to reduce the impact to acceptable levels to allow a useful project to be applied. Risks to privacy need to be addressed by identifying what actions could be taken to mitigate these.

7.26 Privacy solutions are assessed to ensure they are proportionate to the aims of the project by balancing the project outcomes against the impact on individuals. Any privacy solutions identified should be recorded to state whether the risk has been eliminated, reduced or simply accepted. The Constabularies' DPIA template includes a table to record any mitigation factors and suggested privacy solutions.

Sign off and record the DPIA outcomes

7.27 The privacy risks should be signed-off at an appropriate level. This can be done as part of the wider project approval. The Risk Appetite Statement will inform the project team when they may sign off a risk as being acceptable to the Constabularies, by virtue of it being within the national risk appetite. If a risk is outside of the risk appetite then it must be escalated to the SIRO for a decision on whether to accept the risk; invest in mitigating the risk or avoid the risk.

7.28 The project team should ensure that all risk decisions are taken demonstrably in accordance with the Information Risk Management Policy and the Risk Appetite Statement.

7.29 The DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

7.30 It is recommended practice for public authorities covered by the Freedom of Information Act 2000 (FOIA) to include DPIA reports in their publication scheme under Section 19 of FOIA. Publishing a DPIA report will improve transparency and accountability, and lets individuals learn more about how a project affects them.

Intergrating and reviewing of the DPIA

7.31 The agreed privacy solutions should be integrated back into the project plan. This will need to happen whilst the project is still in the development and early implementation stages to ensure that the recommended steps are delivered correctly and produce the required outcome.

7.32 The review of privacy outcomes should be built into existing project processes. If the project aims change and progress, then the DPIA screening questions should be revisited to check the DPIA is still appropriate and the results fed back into the project.

7.33 The Compliance Officer will be able to offer advice and guidance on privacy concerns during the project lifecycle and any issues which may arise in the future.

7.34 The signed DPIA will be centrally recorded and retained by the Compliance team and also documented within the Information Asset Register (IAR) against the applicable asset. The retention of records will be in accordance with the Constabularies' Review, Retention and Deletion (RRD) policy.

8. Who to Contact about this Policy

8.1 Questions regarding this policy and its operation should initially be referred to the Compliance Officer:

- Suffolk Constabulary, Police Headquarters, Martlesham Heath, Ipswich, IP5 3QS. Tel 01473 613500
- Norfolk Constabulary, Operations and Communications Centre, Jubilee House, Falconers Chase, Wymondham, Norfolk, NR18 0WW.

Appendix A – What is meant by Privacy?

Privacy in its basic sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy – the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuses of such information.

Privacy risk is the risk of harm arising through an intrusion into privacy. Some of the ways this risk can arise is through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely.

Understanding privacy risk requires an understanding of the relationship between an individual and the organisation. Factors that can have a bearing on this include:

- Reasonable expectations of how the activity of individuals will be monitored.
- Reasonable expectations of the level of interaction between an individual and an organisation.
- The level of understanding of how and why particular decisions are made about people.

Public bodies need to be aware of their obligations under the Human Rights Act 2000. Article 8 of the European Convention on Human Rights guarantees a right to respect for private life which can only be interfered with when it is necessary to meet a legitimate social need. Organisations which are subject to the Human Rights Act can use a DPIA to help ensure that any actions that interfere with the right to private life are necessary and proportionate.

Appendix B – What is 'High Risk' Processing?

High Risk in the context of DPIAs means the potential for any significant physical, material or non-material harm to individuals. To assess whether something is 'high risk' consideration needs to be given to the likelihood and severity of any potential harm to individuals. 'Risk' implies a more than remote chance of some harm. 'High risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two. Assessing the likelihood of risk is part of the job of the DPIA.

Other than the processing set out by the GDPR and ICO that automatically require a DPIA to be completed, other factors that might indicate likely high risk are:

- Evaluation or scoring
- Automated decision-making with legal or similar effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- Preventing data subjects from exercising a right or using a service or contract

In most cases, a combination of two of these factors indicates the need for a DPIA however; this is not a strict rule. Decisions not to carry out a DPIA may be able to be justified if it is confident that the processing is nevertheless unlikely to result in high risk, but reasons for such decisions need to be documented. In some cases it may be necessary to complete a DPIA if only one factor is present and it is good practice to do so.

Appendix C – Compliance with the Data Protection Principles

Referring to the following during the DPIA process will assist in identifying where there is a risk that the project will fail to comply with the Data Protection Act.

Principle One

Personal data must be fairly and lawfully processed

- Have you identified the purpose of the project?
- How will you tell individuals about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

Principle Two

Personal information must be processed for limited purposes

- Does your project plan cover all of the purposes for processing personal data?
- Have you identified potential new purposes as the scope of the project expands?

Principle Three

Personal information must be adequate, relevant and not excessive

- Is the quality of the information good enough for the purposes it is used?
- Which personal data could you not use, without compromising the needs of the project?

Principle Four

Personal information must be accurate and up to date

- If you are procuring new software does it allow you to amend the data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle Five

Personal information must not be kept for longer than is necessary

- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software that will allow you to delete information in line with your retention periods?

Principle Six

Personal information must be processed in a manner that ensures appropriate security

- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?
- Will the project require you to transfer data outside of the EEA?
- If you will be making transfers, how will you ensure that the data is adequately protected?