STRATEGIC PLANNING, PERFORMANCE AND COMMUNICATIONS

INFORMATION GOVERNANCE

DATA PROTECTION IMPACT ASSESSMENT GUIDANCE

Author/Role	Carol Wade, Information Governance Manager
Date of Risk Assessment (if applicable)	Risks added to Corporate Risk Register
Date of Equality Impact Assessment	Yes
Date of Impact Assessment (commenced)	N/A
Date of Impact Assessment (concluded)	N/A
Quality Control (name)	Morag Allan, Records Management Officer
Authorised (name and date)	Mark McAteer, Director SPPC – 2 May 2018
Last reviewed (name and date)	N/A
Date for Next Review	May 2019

SCOTTISH FIRE AND RESCUE SERVICE
Working together for a safer Scotland

STRATEGIC PLANNING, PERFORMANCE AND COMMUNICATIONS

INFORMATION GOVERNANCE

DATA PROTECTION IMPACT ASSESSMENT GUIDANCE

1. INTRODUCTION

The EU General Data Protection Regulation (GDPR) represents a significant change in the data protection compliance regime for data controllers and data processors including SFRS.

Information and data is an important and valuable asset to any organisation and this includes the personal data we hold on staff or those who rely upon us to keep them safe. Personal data may be used for many different reasons, for example staff administration, the provision of goods or services to customers, strategies, prevention of money laundering, a revenue stream, etc.

The exercise of proper control and management of personal data is fundamental to ensure, and be able to demonstrate, our compliance with the GDPR. By taking a positive approach, and embracing the changes, we will improve our records management, enhance how we use data to improve how we work and in doing so increase the trust individuals and communities place in us.

The new regulations place a greater focus on accountability which means, in addition to being compliant with data protection principles, organisations will have a duty to document what they do with personal data. This will include having a register of all processing, documenting policies and procedures, and ensuring there are appropriate records in relation to information sharing practices, privacy impact assessments and breach management.

2. GUIDANCE

2.1 What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of our accountability obligations under the GDPR and, when done properly, helps us assess and demonstrate how we comply with all of our data protection obligations.

It does not have to eradicate all risk, but should help us minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve.

DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.

There are various controls which will need to be considered. These will include identifying the minimum amount of personal data required, managing access, and providing appropriate security, ensuring that data subjects know what will happen to their data, and deleting it or using anonymisation techniques when it is no longer required.

DPIAs provide evidence that we have considered data protection principles when designing processes that handle personal data. They document that we've tried to do the right thing. Under GDPR, DPIAs which relate to high risk processes will need to be authorised by the Information Commissioner's Office. Please contact the Information Governance Team if you have any queries re this.

2.2 Why are DPIAs important?

DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to €10 million, or 2% global annual turnover if higher.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations.

However, DPIAs are not just a compliance exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both individuals and our organisation.

It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as we can. In some cases, the consultation process for a DPIA gives them a chance to have some say in the way their information is used. Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why we are using their information.

In turn, this can create potential benefits for our reputation and relationships with individuals. Conducting a DPIA can help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations.

There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on. A DPIA can also reduce the ongoing costs of a project by minimising the amount of information we collect where possible, and devising more straightforward processes for staff.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within our organisation and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a 'data protection by design' approach.

2.3 How are DPIAs used?

A DPIA can cover a single processing operation, or a group of similar processing operations. You may even be able to rely on an existing DPIA if it covered a similar processing operation with similar risks. A group of controllers can also do a joint DPIA for partnership working or an industry-wide initiative.

For new technologies, you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans. You can use an effective DPIA throughout the development and implementation of a project or proposal, embedded into existing project management or other organisational processes.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

2.4 DPIAs – changes to existing systems

It is important to remember that DPIAs are also relevant if you are planning to make changes to an existing system. In this case, you must ensure that you do the DPIA at a point when there is a realistic opportunity to influence those plans.

Quote from Recital 84 of GDPR:

'the outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation.'

In other words, a DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It is vital to integrate the outcomes of your DPIA back into your project plan. You should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an ongoing basis. You need to keep it under review and re-assess if anything changes.

In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your DPIA assesses any new risks. An external change to the wider context of the processing should also prompt you to review your DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing you do or the vulnerability of a particular group of data subjects.

2.5 What kind of risk do they assess?

There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. Article 35 says that a DPIA must consider 'risks to the rights and freedoms of natural persons'. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

2.6 What does 'significantly affect' mean?

The GDPR does not define the concept of a legal or similarly significant effect. However, Article 29 working party guidelines on this phrase in the context of profiling provisions give some further guidance.

In short, it is something that has a noticeable impact on an individual and can affect their circumstances, behaviour or choices in a significant way.

A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

Decisions that have little impact generally could still have a significant effect on more vulnerable people, such as children.

2.7 Are there any exceptions?

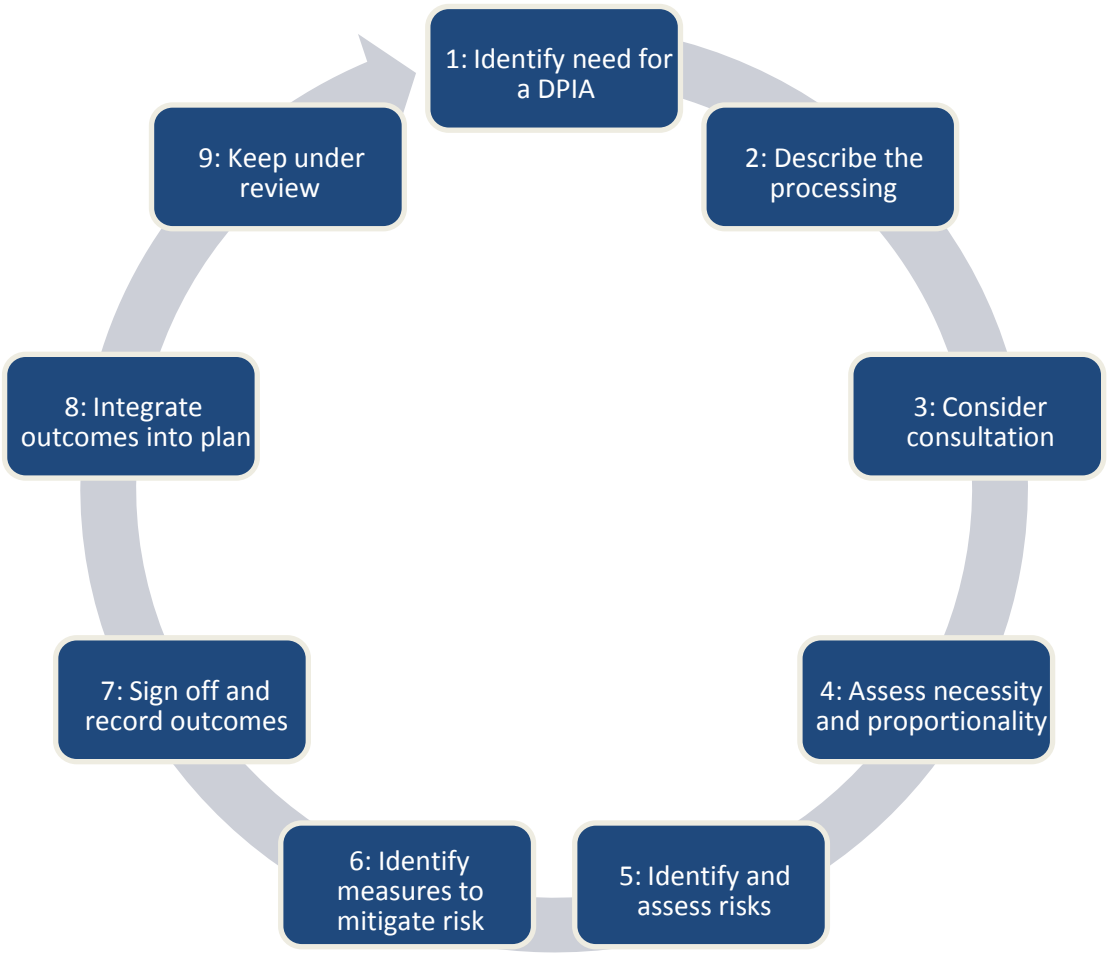
You may not have to carry out a DPIA if:

- **You are processing on the basis of legal obligation or public task.** However, this exception only applies if:
    - you have a clear statutory basis for the processing
    - the legal provision or a statutory code specifically provides for and regulates the processing operation in question
    - you are not subject to other obligations to complete DPIAs, such as those required by Cabinet Office for consideration of information governance risks or requirements derived from specific legislation, such as Digital Economy Act 2017
    - a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted. This may not always be clear, and in the absence of any clear and authoritative statement on whether such an assessment was conducted we recommend that you err on the side of caution and conduct a DPIA to ensure you consider how best to mitigate any high risk.
- **You have already done a substantially similar DPIA**. You need to be confident that you can demonstrate that the nature, scope, context and purposes of the processing are all similar.

2.8 How do we carry out a DPIA?

In brief….

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



You must seek the advice of the Information Governance Team. You should also consult with individuals and other stakeholders throughout this process.

2.9 Is there a template we can use?

SFRS have prepared a template for you to use which can be found at the following link - DPIA Template.

2.10 Who is responsible for the DPIA?

The project or process lead has responsibility for carrying out DPIAs within each Directorate/Department/Function/Station; however, these must be approved by the Information Governance Team to ensure full compliance before signing.

2.11 Who should be involved in the DPIA?

- Information Governance Team
- Any processors, and
- Legal advisors or other experts, where relevant

2.12 How do we describe the processing?

Describe how and why you plan to use the personal data. Your description must include 'the nature, scope, context and purposes of the processing'.

The nature of the processing is what you plan to do with the personal data. This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any processors;

- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

The scope of the processing is what the processing covers. This should include, for example:

- 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; and
- the geographical area covered.

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- the source of the data;
- the nature of your relationship with the 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; and
- in due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes;
- whether you have considered and complied with relevant codes of practice.

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

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole.

2.13 Do we need to consult individuals?

You should seek the views of individuals (or their representatives), unless there is a good reason not to.

In most cases, it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals, then you should record this decision as part of your DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

2.14 Do we need to consult anyone else?

If you use a data processor, you may need to ask them for information and assistance. SFRS contracts with processors should require them to assist.

You should consult all relevant internal stakeholders, in particular, anyone with responsibility for information security.

In some circumstances, you might also need to consult the ICO once you have completed your DPIA. The Information Governance Team will assist you with this decision.

2.15 How do we assess necessity and proportionality?

The Information Governance Team will be able to provide advice in this area. You should consider:

- Do your plans help to achieve your purpose?
- Is there any other reasonable way to achieve the same result?

You should include how you ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, you should include relevant details of:

- your lawful basis for the processing;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals rights;
- measures to ensure your processors comply; and
- safeguards for international transfers.

2.16 How do we identify and assess risks?

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular, look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy 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 of pseudonymised data; or
- any other significant economic or social disadvantage.

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

You must make an 'objective assessment' of the risks using a structured matrix to assess likelihood and severity of risks:

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

You might also want to consider your own corporate risks, such as the impact of regulatory action, reputational damage or loss of public trust.

2.17 How do we identify mitigating measures?

Against each risk identified, record the source of that risk. You should then consider options for reducing that risk. For example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;

- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- adding a human element to review automated decisions;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks. You should ask the Information Governance Team for advice.

Record whether the measure would reduce or eliminate the risk. You can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

2.18 How do we conclude our DPIA?

You should then record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether you need to consult the ICO.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable, given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.

As part of the sign-off process, you must ask the Information Governance Team to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons.

You should also record any reasons for going against the views of individuals or other consultees.

2.19 What happens next?

You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project management process to ensure these are followed through.

You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

All DPIAs, once approved, will be published on the iHub to aid transparency and accountability. This helps foster trust in our processing activities, and improve individuals' ability to exercise their rights. If you are concerned that publication might reveal commercially sensitive information, undermine security or cause other risks, you should consider whether you can redact (black out) or remove sensitive details, or publish a summary. Public authorities need to consider their freedom of information obligations, as privacy impact assessments are included in the definition documents for publication schemes for many public authorities.

You need to keep your DPIA under review, and you may need to repeat it, if there is a substantial change to the nature, scope, context or purposes of your processing.

3. ASSOCIATED DOCUMENTS / REFERENCES

General Data Protection Regulations (GDPR) Policy (available when legislation is live)

Data Protection Impact Assessment (DPIA) Template