**[Stafford Fuels Limited]** **Data Protection Impact Assessment**[[1]](#footnote-1)

[Date]

The purpose of this document is to: (i) consider the privacy risks and the potential impact upon the relevant individuals [(including employees)] in respect of the proposed use of [insert description of new systems/technology]; and (ii) to describe the mitigations that will be in place to minimise those risks and to minimise any negative impact from a data protection compliance perspective.

This document is written in the context of [both the current Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such personal data and] the EU General Data Protection Regulation (“**GDPR**”)[, due to come into force from 25 May 2018][[2]](#footnote-2).

1. Introduction and methodology
   1. [INSERT ANY RELEVANT BACKGROUND TO THE PROPOSED SYSTEM/TECHNOLOGY/PROCESS – E.G. IS IT NEW OR AN UPGRADE? WHICH ENTITY/ COMMITTEE HAS OR IS TAKING RESPONSIBILITY FOR IT? ETC].
   2. [Stafford Fuels Ireland Limited (“**Stafford Fuels**”)][[3]](#footnote-3) has prepared this Privacy Impact Assessment (“**PIA**”) in respect of its [use/proposed use] of [insert description of relevant systems/technology/process] in [insert relevant location]. In order to prepare this PIA, a questionnaire was completed by [relevant Stafford Fuels business] which related to the [manner/proposed manner] in which [system/technology/process] is [used/to be used]. This helped to identify privacy risks prior to preparing the PIA.
   3. PIA’s are important as they allow us to anticipate and address the likely privacy impact of projects, processes, systems and technologies, in order to identify privacy related issues, develop solutions, and ensure that such issues are addressed appropriately in a manner consistent with statutory obligations and company policies.
   4. This PIA is a statement of Stafford Fuels commitment to integrating a “privacy by design” approach to the introduction of systems, processes and technology that can impact on the privacy of [Stafford Fuels employees as well as third party individuals with or through whom we do business].
   5. Stafford Fuels, as a data controller, places a high priority on the protection of the privacy of its [employees and such third parties]. It demonstrates its commitment to a “*privacy by design*” approach through the implementation of appropriate technical and organizational measures to ensure by default only personal data which is necessary for each specific purpose is processed. This applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility.
   6. Statutory obligations under the GDPR and the local data protection laws place obligations on Stafford Fuels to protect the privacy of personal data under its control.
2. Use and functionality of [System/Technology/Process]
   1. [Use/Proposed Use of System/Technology/Process]

[Insert description of how Stafford Fuels uses or proposes to use the relevant system/technology/process setting out the purposes for which the system/technology/process is being implemented]

* 1. Functionality, nature and scope of personal data collected

[If technology based, describe the functionality of the technology in terms of the scope and type of personal data it is set up to collect. If it is a new process, describe how and what personal data it will collect. Describe the types of Special Categories of Personal Data[[4]](#footnote-4) (if any) which will be processed in the context of the [system/technology/process]**]**

* 1. Data transfers

[Note whether this personal data is transferred or accessible from outside the EEA]. This transfer of personal data [is/shall be] governed by [European Commission approved model contract clauses/insert description of relevant transfer mechanism].

1. Data protection and privacy
   1. This section of the document details the main data protection responsibilities relating to the [system/technology/process], and how the design and manner of operation of [system/technology/process] mitigate the associated risks. Key risks are highlighted at the end of each section along with a description of the relevant mitigations. All such risks are risks to individuals, but may also, due to risks of non-compliance with relevant legislation, be corporate risks to Stafford Fuels.
   2. [NOTE WHETHER THE RELEVANT TECHNOLOGY/SYSTEM/PROCESS IS ALREADY SUBJECT TO RELEVANT Stafford Fuels POLICY OR PROCEDURE.]
2. Fair obtaining
   1. Fair processing of the personal data [being/to be] processed by [system/technology/process] is achieved by[[5]](#footnote-5):
      1. [publishing information about its use on our [intranet]];
      2. Stafford Fuels security policies (which include information on [system/technology/process]) are made available for all employees on the [intranet];
      3. [Stafford Fuels employment contracts include a data protection clause explaining when and how Stafford Fuels processes personal data and the [system/technology/process] is within scope of such clause]; and/or
      4. [other individual customers and individual third parties are informed through [Stafford Fuels contracts/policies/terms and conditions etc.]

|  |  |
| --- | --- |
| **Key risks relating to fair obtaining** | **Mitigation** |
| [e.g.is there a risk that an individual would not be aware of how his/her personal data is being used] | [Explain how relevant measures taken to achieve fair processing and to mitigate this risk]. |

1. Purpose of collected and shared personal data

The main purposes of [system/technology/process] are as follows:

* + [explain purposes]

|  |  |
| --- | --- |
| **Key risks relating to purpose[[6]](#footnote-6)** | **Mitigation** |
| It is possible that personal data will be captured through the [system / technology / process] which personal data is ultimately not relevant to achieving the above purposes. | [Explain extent of access to personal data, how long it is retained, how irrelevant personal data is deleted, etc.] |

1. Use and disclosure of information
   1. As a general rule, access to any personal data is limited to a [small number of individuals] in a [specific office/company] who have the requisite level of clearance. [Personal data is not shared with any third parties].
   2. [Note any risks from a law enforcement perspective e.g. are there any legislation that could require the disclosure of the personal data to law enforcement officials/regulators, etc.?]

|  |  |
| --- | --- |
| **Key risks relating to use and disclosure** | **Mitigation** |
| Personal data might be leaked if there was a data breach or hack of some kind. | [Insert security measures explaining how such breaches are guarded against e.g. state of the art security, etc.] |

1. Security

[Explain security measures in place to control and protect access to and storage of the personal data]

|  |  |
| --- | --- |
| **Key risks relating to security** | **Mitigation** |
| [Insert any risks that are not already addressed above in section 6] | [Insert relevant mitigating security measures, for example, encryption etc.] |

1. Adequacy and relevance

Adequacy and relevancy are key considerations for the lawful processing of personal data. In accordance with good data protection practice, it is worth considering whether there is an equally effective way for Stafford Fuels to achieve its goals without using [system/technology/process]. [On balance, we do not believe that there is and the deployment of [system/technology/process] is necessary because [insert purpose]].

|  |  |
| --- | --- |
| **Key risks relating to adequacy and relevance** | **Mitigation** |
| Personal data that is not relevant to the purposes of the [system/technology/process] is captured. | ⚫ |

1. Accuracy

[Consider whether any personal data collected is likely to be inaccurate and how that would be identified and remedied.]

|  |  |
| --- | --- |
| **Key risks relating to accuracy** | **Mitigation** |
| ⚫ | ⚫ |

1. Retention

Data protection law provides that personal data shall not be kept for longer than is necessary for the purpose(s) for which it was obtained.

|  |  |
| --- | --- |
| **Key risks relating to retention** | **Mitigation** |
| This principle of data protection law would be breached if the personal data was, without reason, held indefinitely or for a long period of time. | [insert relevant retention period and rationale behind that retention period] |

1. Right of access
   1. Data protection law provides for a right to establish the existence of personal data and a right of access to personal data.
   2. This law also allows for certain restrictions to the right of access. [The most relevant one in the context of [system/technology/process] is that the right of access may be restricted where [insert any relevant exemption or limitation and how it is relevant].

|  |  |
| --- | --- |
| **Key risks relating to right of access** | **Mitigation** |
| Information held on an individual is not released following an access request, due to a determination by Stafford Fuels that one of the exceptions to the right of access applies. | The default policy will be to always release information following receipt of a valid access request; however Stafford Fuels will apply the exemptions where it feels that it is necessary / appropriate to do so. |

1. **Right to rectification or erasure and right to object**
   1. Data protection law provides for a right for an individual to have rectified or, where appropriate, blocked or erased any personal data relating to him/her in respect of which the data controller has breached its obligations in relation to fair collection and processing, adequacy and relevance, accuracy, etc. The law also provides for a right to object to processing likely to cause unwarranted damage or distress, subject to certain exceptions.
   2. Article 17 of the GDPR has introduced a more explicit “right to be forgotten” where, under certain grounds, an individual can instruct a data controller to erase personal data, and Article 21 provides for a right to object to processing. An individual can withdraw consent for or object to processing. However, a data controller may continue to process personal data, despite such a withdrawal or objection, if the data controller can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject. A strong argument could be made that the legitimate grounds for the processing of personal data concerning [insert relevant purpose of system/technology/process] generally overrides the objections of data subjects to such processing.

|  |  |
| --- | --- |
| **Key risks relating to erasure, rectification and the right to object** | **Mitigation** |
| An individual makes a request for erasure but Stafford Fuels, as data controller, determines that there has not been a contravention the relevant law and / or it is in the legitimate interests to continue. | The individual may apply to their local data protection regulator for review. [note any relevant retention period in place and whether it is short enough to constitute a mitigating factor] |

1. Residual/Unmitigated Risks

Where a data protection impact assessment indicates that the processing of the personal data would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and Stafford Fuels is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period.

1. **Explanatory Note:** The GDPR requires that, where processing operations are likely to result in a high risk to the rights and freedoms of individuals, the relevant Stafford Fuels company that is the data controller in the relevant instance, should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature and severity of that risk. The outcome of the assessment should be used to determine the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with the GDPR. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation with the relevant data protection regulator should take place prior to the processing/use/deployment of the system or process under review.

   The GDPR notes that this should, in particular, apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or global level and which could affect a large number of data subjects and which are likely to result in a high risk. For example this may arise where a new technology is used on a large scale such that there is a high risk to the rights and freedoms of data subjects. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific individuals following any evaluation of personal aspects relating to those individuals based on profiling or following the processing of sensitive or criminal data. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, such as CCTV or other instances viewed as high risk by a regulator, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale.

   There are circumstances where a single DPIA could cover more than a single project, for example where Stafford Fuels or several group companies intend to establish a common application or processing platform. Where appropriate, Stafford Fuels should seek the input from any relevant service providers (e.g. relevant platform provider) in completing the DPIA. [↑](#footnote-ref-1)
2. **Note**: Amend accordingly to time at which the DPIA is being undertaken. If post 25 May 2018, do not include the reference to the EU Directive or the due date for commencement of the GDPR. [↑](#footnote-ref-2)
3. Amend as appropriate [↑](#footnote-ref-3)
4. **Note**: “**Special Categories of Personal Data**” are defined in the GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. [↑](#footnote-ref-4)
5. **Note to draft**: Amend/update as required. [↑](#footnote-ref-5)
6. **Note to draft**: These are examples of relevant risks. [↑](#footnote-ref-6)