**Stafford Fuels Limited**

**Personal Data**

**Security Breach Procedure**

**FOR INTERNAL USE ONLY**

**Important Notice**

It is crucial for all Stafford Fuels employees (and contractors) to immediately report any potential or suspected Data Breach (as defined in this Procedure) to the Managing Director by phone and email – contact details are set out in paragraph 3 of this Procedure. If unsure whether an incident is a Data Breach or not please refer to the guidance set out in this Procedure and consult with the Managing Director

1. Introduction
   1. **Stafford Fuels Limited** (“**Stafford Fuels**”) is a Data Controller[[1]](#footnote-1) as outlined in Stafford Fuels privacy policy, for the purposes of the General Data Protection Regulation (Regulation (EU) 2016/679) (the “**GDPR**”). The GDPR imposes obligations on Data Controllers and processors to process Personal Data (as defined below) in a manner that ensures the security, confidentiality and integrity of the Personal Data by implementing appropriate technical and organisational measures. In the event of a Data Breach (as defined below) that is likely to cause a risk to individuals the GDPR requires mandatory notification to the Data Protection Commission (the “**DPC**”) and, in some cases, an additional communication to the affected individuals. This Personal Data Security Breach Procedure (the “**Procedure**”) describes the process for identifying, escalating, reporting and recording suspected or actual Data Breaches involving Personal Data in accordance with Stafford Fuels GDPR obligations.
   2. The purpose of this Procedure is to ensure that Stafford Fuels manages and contains any Data Breach quickly so that the impact of the Data Breach can be minimised and any legal obligation to report the Data Breach to a regulator and/or any individual(s) affected by the Data Breach (in accordance with the GDPR) can be complied with in good time. This Procedure is also intended to enable Stafford Fuels to take appropriate measures to reduce the risks for affected individuals.
2. Who does this Procedure apply to?
   1. This Procedure applies to all employees of Stafford Fuels. This Procedure also applies to independent contractors, agency temps and staff seconded to Stafford Fuels. Together all employees, to whom Personal Data is disclosed, and contractors, agency temps and staff seconded to Stafford Fuels are referred to in this Procedure as “**Personnel**”. All Personnel should be provided with and read a copy of this Procedure.
3. What is Personal Data?
   1. “**Personal Data**” is any information relating to an identifiable living individual. A person is identifiable if he/she can be identified directly or indirectly, for example by reference to an identifier such as a name, address, date of birth, telephone number, account number, job title, photo, IP Address, etc. If in doubt as to whether any specific information or data may constitute Personal Data, consult with the Managing Director.
4. What is a Personal Data Breach?
   1. The GDPR defines a ‘*personal data breach*’ as “*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*” (“**Data Breach**”). A Data Breach occurs when there is any unauthorised or accidental disclosure, loss or any other form of unauthorised, accidental or unlawful collection, use, recording, storing or distributing (each being a form of “**Processing**”) of Personal Data. Examples of Data Breaches may include but are not limited to:
      1. loss, theft or misplacement of IT equipment or devices containing Personal Data e.g. smartphone, laptop or USB key;
      2. loss, theft or misplacement of briefcase or folder containing Personal Data in physical hardcopy form;
      3. human error resulting in email or post containing Personal Data being sent to an unintended recipient;
      4. unauthorised access to automated or manual Personal Data as a result of a break-in to an office or building on any Stafford Fuels premises;
      5. unauthorised access to Personal Data as a result of a breach of access controls;
      6. an attack by a “Hacker”, i.e. unauthorised access to Stafford Fuels computer network, which may consist of a deliberate interruption to IT network services or penetration of the IT network or system, by an unauthorised party with the intention of obtaining information, destroying data or preventing access to data;
      7. unforeseen circumstances such as a flood or fire, in particular where Personal Data is not accessible either temporarily or permanently;
      8. unauthorised access to Personal Data where information is obtained by deception; and
      9. in certain circumstances, where there is a loss of access to or availability of Personal Data (temporarily or permanently), for example where Personal Data has been deleted either accidentally or by an unauthorised person and the data cannot be restored.
   2. Whether the incident (the “**Data Incident**”) giving rise to the suspected Data Breach involves Personal Data must be determined on a case-by-case basis. If a Data Incident does not involve Personal Data, it is not a Data Breach. Furthermore, not all Data Incidents involving Personal Data will be Data Breaches. For example, the loss or compromise of Personal Data may not qualify as a Data Breach where:
      1. there is no risk to the individuals, their rights or freedoms, resulting from the Data Breach;
      2. the Personal Data is securely encrypted or anonymised such to make the Personal Data unintelligible; and/or
      3. there is a full, up-to-date back-up of the Personal Data (in cases of accidental destruction).
5. Personnel obligation to report Data Incidents to the Managing Director
   1. It is vital that all Data Incidents are immediately reported to the Managing Director as soon as they are identified. It is the role of the Managing Director to ascertain whether the Data Incident is in fact a Data Breach. The Managing Director contact details are as follows:

|  |  |
| --- | --- |
| Name | Andy Maher |
| Email | [Andy.maher@staffordfuels.ie](mailto:Andy.maher@staffordfuels.ie) |
| Phone | 0876873985 |

* 1. Prompt reporting of any Data Incidents to the Managing Director is crucial to ensure compliance with the GDPR, which contains a number of action points that must be put into immediate effect when Stafford Fuels is alerted or notified of a suspected or potential Data Breach.
  2. These detailed action points are comprised in the **Data Breach Response Plan** set out in Appendix 1. However, for Personnel the most important obligation to be aware of is that any Data Incident should be reported immediately to Stafford Fuels Managing Director. In implementing the **Data Breach Response Plan**,the Managing Director will investigate the Data Incident, liaising with the relevant departments as necessary to assess whether it is a Data Breach and the level of risk to the affected individuals, consider containment measures and determine whether: (i) a notification to the DPC; and/or (ii) a communication to the affected individuals is required.
  3. While it is important to note that not all Data Incidents will necessarily involve Personal Data, and will not require notification to the DPC, all Personnel should note that all loss/theft/misplacement of IT equipment must be reported to the Managing Director and the IT Department.

1. Outsourced Activities
   1. The GDPR requires that all Data Breaches must be reported to the relevant Data Controller without undue delay[[2]](#footnote-2) as soon as the Data Processor[[3]](#footnote-3) becomes aware of the incident. Where processing of Personal Data is outsourced to a third party, it is the responsibility of the Head of Unit to ensure that each Data Processor engaged by Stafford Fuels: (a) has a contractual obligation to notify Stafford Fuels on becoming aware of any suspected Data Breach relating to Personal Data they are processing on behalf of Stafford Fuels; and (b) has been advised that they must bring any suspected Data Breaches relating to Personal Data they are processing on behalf of Stafford Fuels to the attention of Stafford Fuels immediately as soon as they are identified.
2. Making a Report to the Office of the Data Protection Commissioner
   1. The Managing Director is responsible for making reports to the DPC in accordance with the Data Breach Response Plan and will act as liaison between the DPC and the relevant department in relation to requests for detailed written reports or any subsequent investigation by the DPC.
3. Record of Personal Data Security Breaches in Data Breach Log
   1. In accordance with the **Data Breach Response Plan** (set out in Appendix 1), the Managing Director is responsible for keeping a written record of all potential or suspected Data Breaches that are notified to him/her (including those that are not notified to the DPC or the affected individuals). For this purpose he/she, in conjunction with the relevant department/employee making the report, will complete the Personal Data Security Breach Incident Report contained in Appendix 3.

**Appendix 1 – Data Breach Response Plan**

1. Step 1: Internal report / report by processor/ escalation
   1. Given the tight timelines within which Data Breaches must be reported to the DPC, it is crucial that all Personnel immediately report any potential or suspected Data Breach to the Managing Director **Timing:** Immediately on alert or notification of suspected/potential Data Breach.
2. Step 2: Initial Investigation
   1. Once reported to the Managing Director, there is a short period (of up to 24 hours[[4]](#footnote-4)) during which Stafford Fuels must determine whether the incident has given rise to a Data Breach or not (see definition above). If the Managing Director determines there has been no Data Breach, proceed to steps 7 and 11.

**Timing:** 0 hrs – 24 hours after initial alert or escalation of suspected/potential Data Breach.

1. Step 3: Risk assessment and containment (simultaneous to step 2):
   1. If the Managing Director determines that incident does or may amount to a Data Breach, the next step is to assess the risks to individuals (for example, identity theft, fraud, reputational damage). This assessment should, in particular, consider the likelihood of risks taking place and the severity of such risks is to be categorised as ***no risk / risk / high risk*** in accordance with the detailed criteria below:
      1. **Type of breach:** A Data Breach may include any unauthorised or accidental disclosure, loss, destruction, damage or any other form of unauthorised, accidental or unlawful access to, collection, use, recording, storing or distributing of Personal Data. What type of Data Breach has or may have occurred? Does the breach consist of a breach of confidentiality relating to Personal Data? Is there a temporary or permanent lack of availability or access to Personal Data and if temporary, how long will it be before it is restored?
      2. **Nature of Personal Data:** Is the relevant Personal Data sensitive in nature? The more sensitive the Personal Data the higher the risk of the Data Breach. The utility of the relevant information may also indicate a higher risk to the affected individuals.
      3. **Scale and volume of Personal Data affected:** The higher the volume of the Personal Data records and the number of individuals potentially affected will usually create a higher risk.
      4. **Ease of identification:** The ease of identifying the relevant individuals based on the Personal Data will likely increase the risk of identity theft, fraud and reputational damage in particular.
      5. **Security measures:** Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact and the data is unintelligible to a third party?
      6. **Containment measures:** Have any containment measures been implemented which mean that the Data Breach is unlikely to present a risk to the individuals affected?
      7. **Other factors:** Other relevant factors in assessing the risk to individuals is whether those individuals affected by the Data Breach have any special characteristics (for example children or vulnerable adults).
      8. **Severity of risk:** Based on the above criteria and any other relevant factors, the Managing Director] should assess the severity of the risk in terms of the potential consequences to the individuals affected by the Data Breach.[[5]](#footnote-5)
      9. **Likelihood of the risk(s) materialising:** Once the Data Breach has occurred, the Managing Director] must objectively assess the likelihood of the potential risks actually materialising[[6]](#footnote-6) and this should form part of the risk assessment.
   2. The assessment of the Data Breach based on the above criteria should be an objective assessment focused on the risks likely to result from the Data Breach. Once it has been established with “a reasonable degree of certainty” that a Data Breach has occurred, Stafford Fuels is considered to be “aware” of the Data Breach[[7]](#footnote-7). Unless the Data Breach is “unlikely to result in a risk to individuals” (having carried out the assessment above) then a notification to the DPC is **mandatory** under the GDPR (see **Step 5**).[[8]](#footnote-8) Consideration should be given as to whether communications in this phase are or should be subject to legal privilege so consult with the Managing Director (and external legal advisors if necessary).

**Timing:** 0 hrs – 24 hours (ideally) provided that any report is made within 72 hours from the end of that initial 24 hour period.

1. Step 4: Containment (simultaneous to step 3)
   1. Simultaneously, Stafford Fuels, with the assistance of the departments (such as the IT Department) and appropriate external advisors, will consider what measures should be taken to contain the Data Breach in order to mitigate the risks to the affected individuals and the adverse effects of the Data Breach. These measures should be implemented without delay.

**Timing:** 0 hrs – until Data Breach has been contained.

1. Step 5: Notification to the DPC
   1. If it has been established that there exists ***a risk*** to the rights and freedoms of individuals as a result of the Data Breach (which may include identity theft, fraud, reputational damage), then Stafford Fuels Managing Director is required to report the Data Breach to the DPC without undue delay and within 72 hours from Stafford Fuels becoming aware of the Data Breach (see **Step 3** above).
   2. If the relevant details surrounding the Data Breach are not clear within the initial 72 hour notification period, an initial notification should be made to the DPC. Subsequent notifications can be made to the DPC in phases. Consideration as to whether a communication to affected individuals is required should be addressed when notifying the DPC.

**Timing:** Within 72 hrs of becoming aware of the breach.[[9]](#footnote-9)

1. Step 6: Notification to individuals affected
   1. Based on the risk assessment carried out in Step 3, where the Managing Director assesses that there is ***a high risk*** to rights and freedoms of individuals as a result of the Data Breach, then the existence of the Data Breach should be communicated to the affected individuals without undue delay. Any such communication should inform the affected individuals on relevant measures that they can take to reduce the risks to them and any negative consequences arising from the Data Breach. Stafford Fuels should determine the most appropriate and effective means of communicating the Data Breach to the affected individuals, if necessary engaging the assistance of communications advisors.

**Timing:** Without undue delay (to be determined on a case-by-case basis and after consultation with the DPC if appropriate).

1. Step 7: Other Notification requirements
   1. Stafford Fuels should consider whether, and seek advice as appropriate, as to whether there are any other relevant notification requirements are required (such as to the Gardaí etc.).

**Timing:** will depend on the Data Breach and the legal advice provided in relation to the Data Breach.

1. Step 8: Further investigation
   1. Certain Data Breaches will require further detailed investigation after the initial investigation period, which may involve external IT, legal and other support, as appropriate to ascertain the full extent of the Data Breach, its causes, likely consequences and in order to effectively contain the breach. The effect of the Data Breach must be monitored and the risks re-evaluated throughout this period. It may be necessary to agree a phased notification program with the DPC in these cases.

**Timing:** After initial 72 hrs (as appropriate).

1. Step 9: Phased notification
   1. Once all relevant details have been obtained in the further investigation phase (see **Step 8** above), Stafford Fuels should consider whether further notification to the DPC is appropriate. For example, a further notification may state that the Data Breach has been effectively contained or that on further investigation, no Data Breach had actually occurred.

**Timing:** After initial notification (as appropriate).

1. Step 10: Post-Breach investigation detailed review and recommendations
   1. Once the Data Breach has been contained and relevant engagement and/or DPC investigations have concluded, Stafford Fuels should conduct a post-Data Breach review including detailed recommendations to be implemented to reduce the recurrence of similar Data Breaches and to ensure that appropriate organisational and technical security measures are put in place.

**Timing:** Once the Data Breach has been contained.

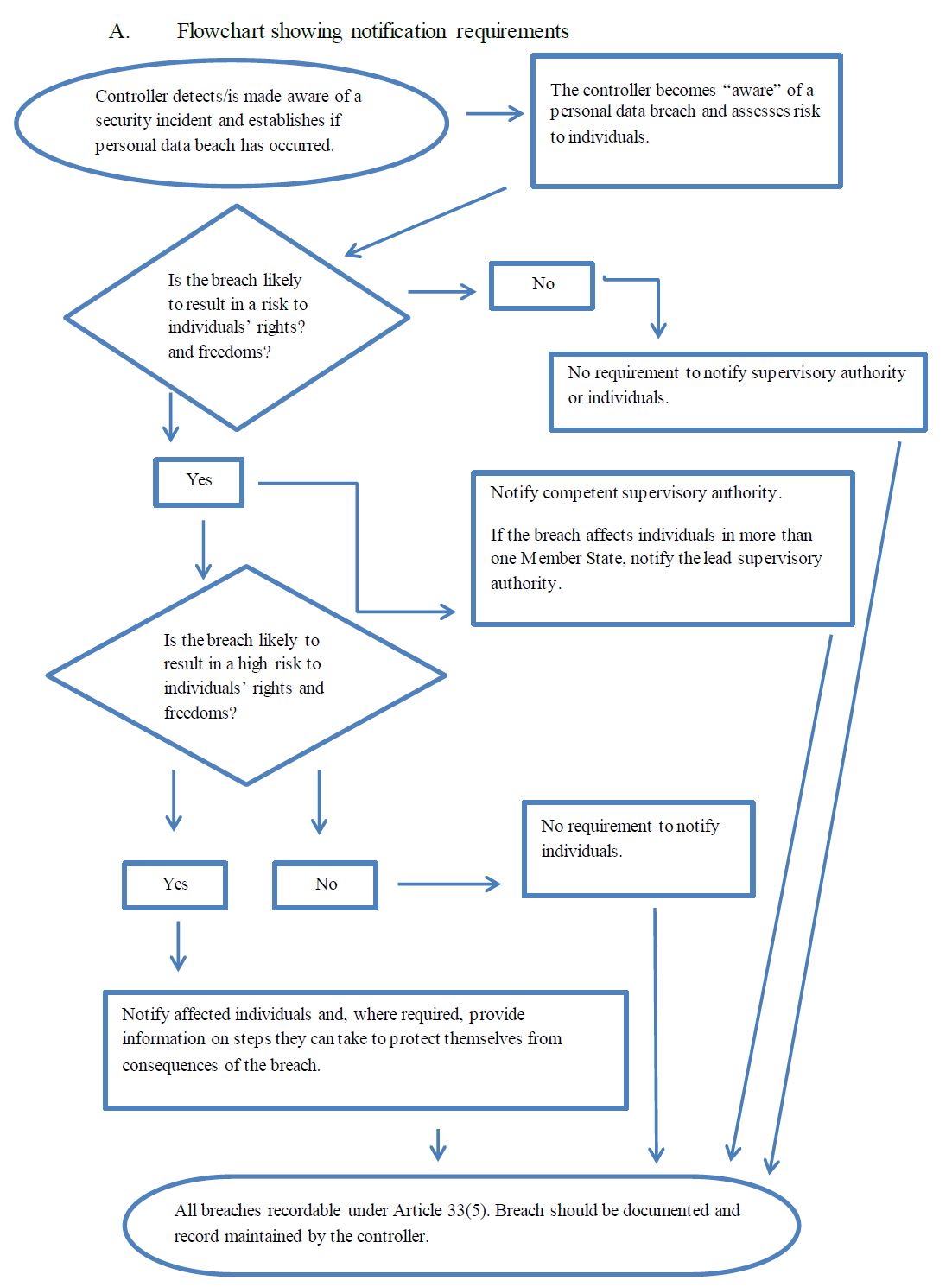
1. Step 11: Recording of Data Breach in Data Breach Log
   1. Stafford Fuels is required to maintain a log of all Data Breaches and Data Incidents (including those not requiring notification to the DPC and/or a communication to individuals). The log entry must specify at least: (i) the facts relating to the Data Breach or Data Incident; (ii) its effects; and; (iii) the remedial action taken by Stafford Fuels. The Article 29 Working Party Guidelines also recommend that any decisions taken not to report a Data Incident to the DPC and/or to communicate it to individuals should also be recorded, including the reasons for such decision (as part of the risk assessment undertaken at **Step 3** above and for accountability purposes).

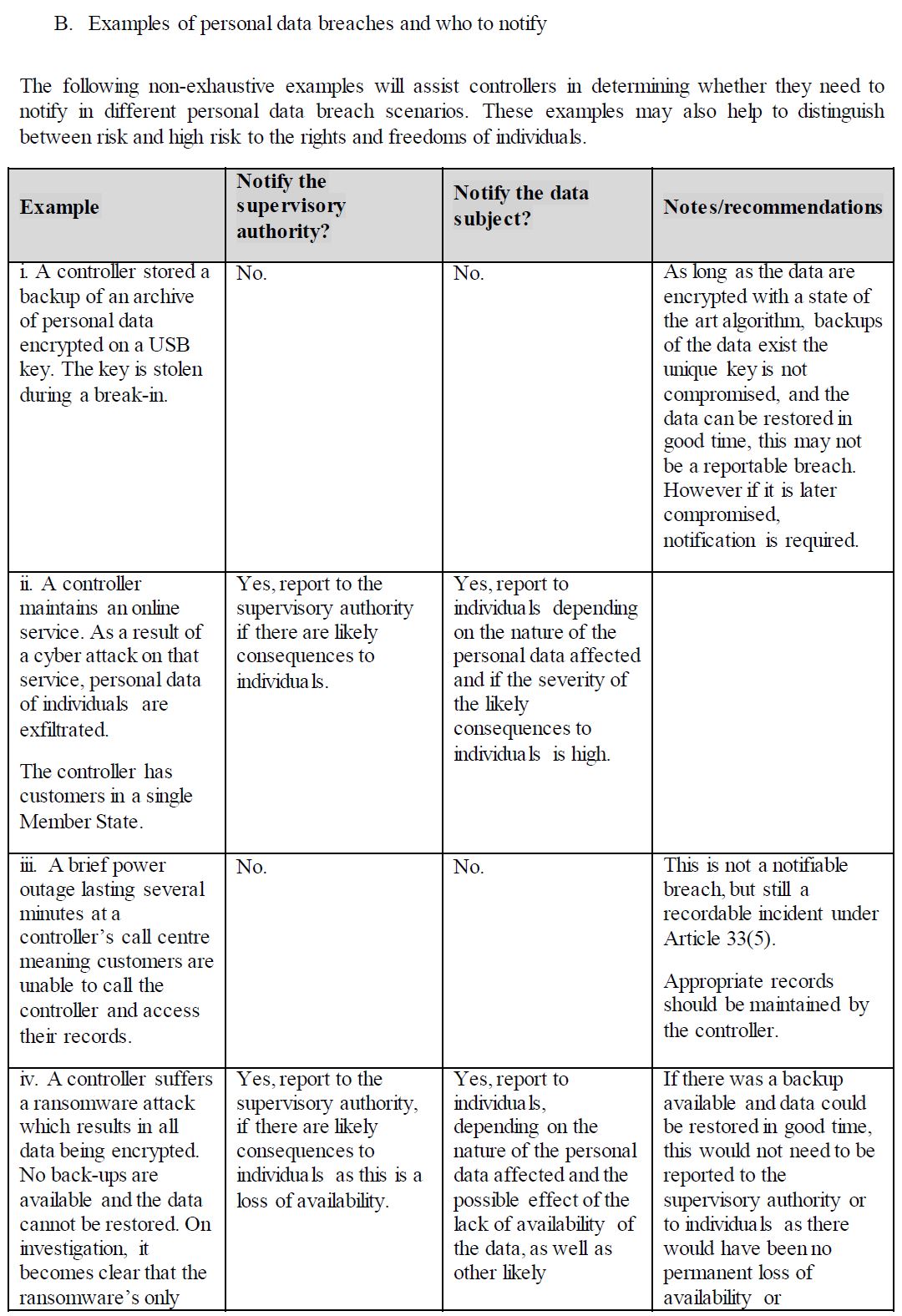
**Timing:** Once the Data Breach has been contained and the investigation is complete.

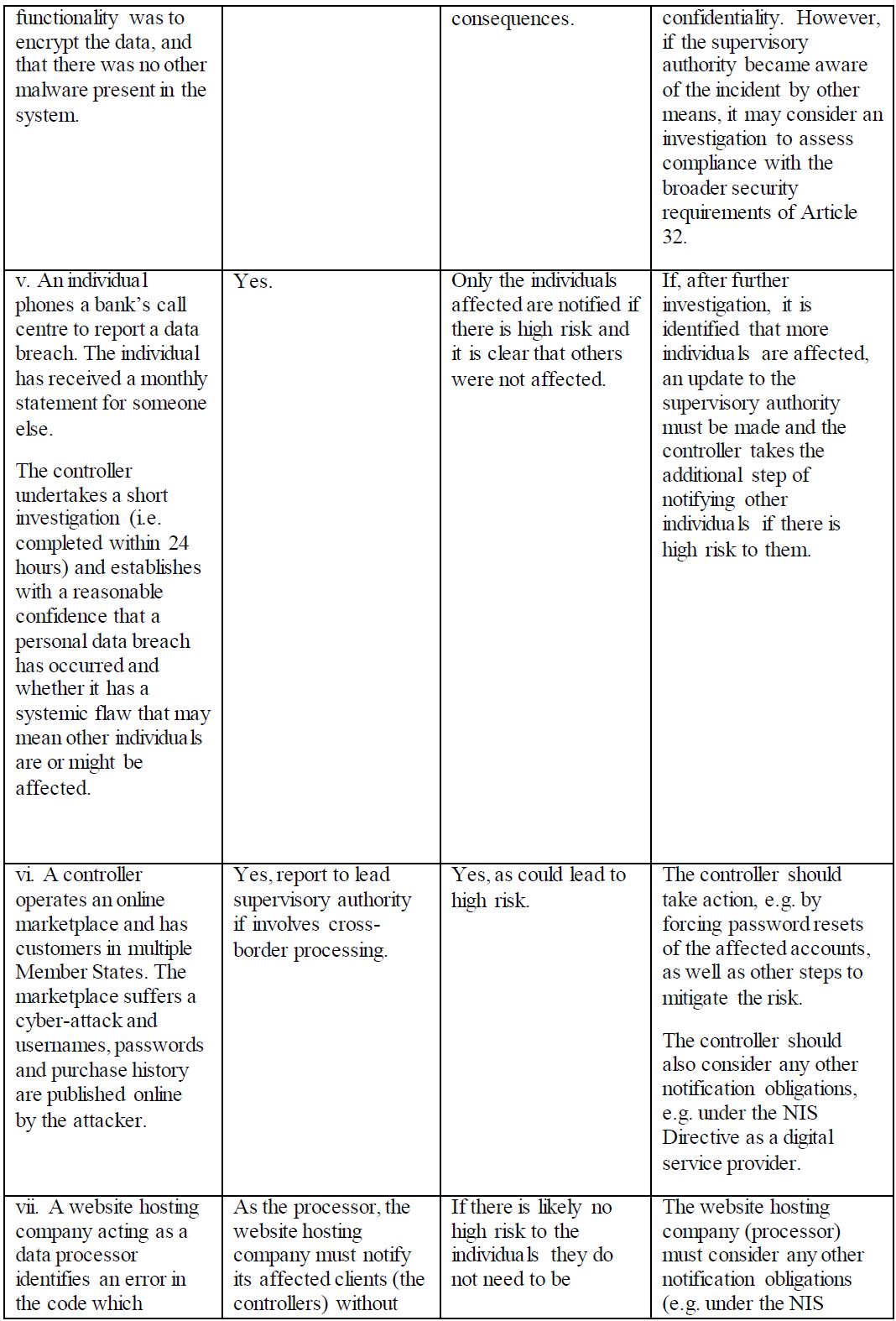
1. Step 12: Implementation of recommendations
   1. The recommendations identified in **Step 10** should be implemented without delay. The recommendations may include revising and updating of data protection and IT security policies and/or technical measures.

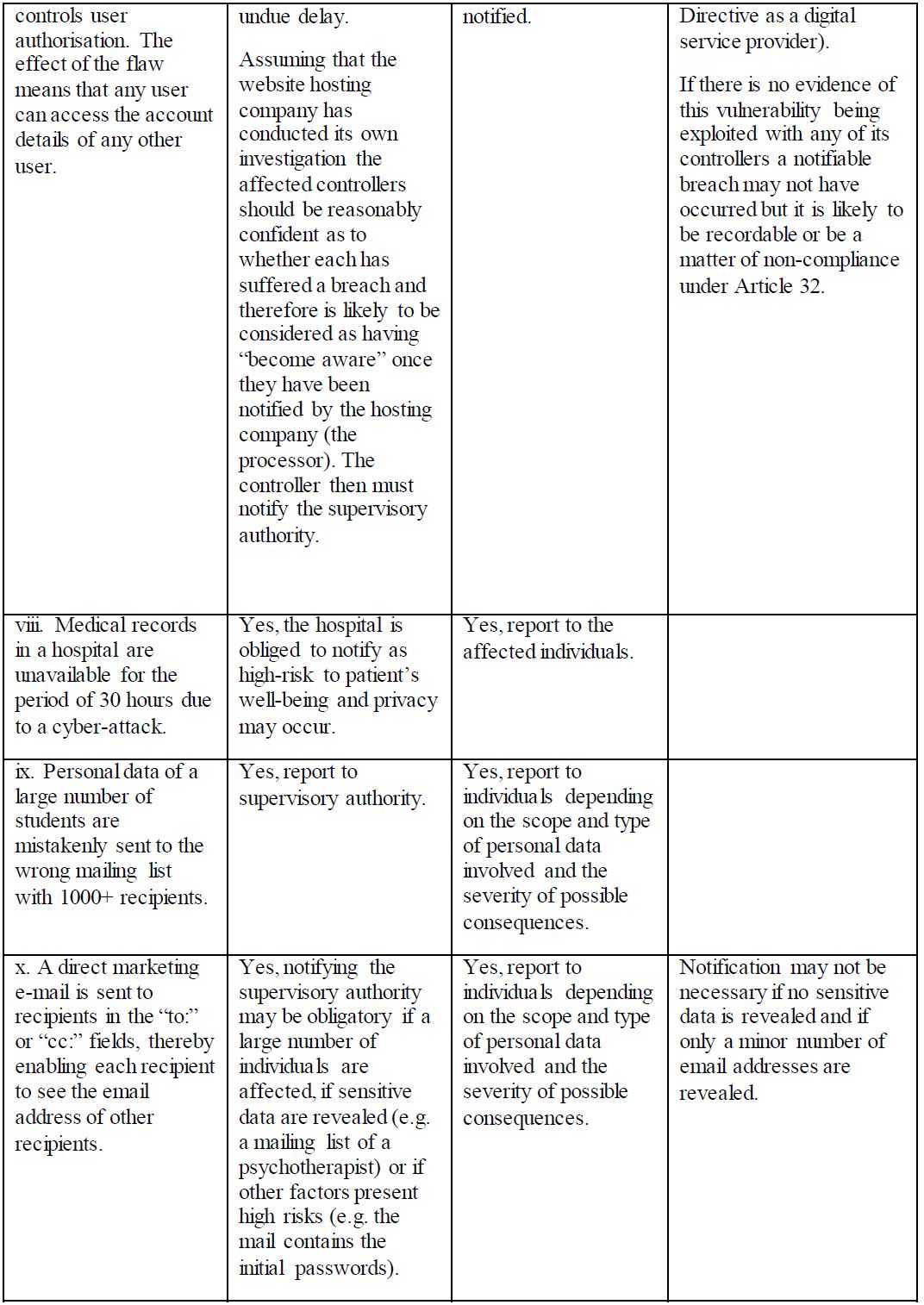
**Timing:** Once the Post-Breach investigation (see **Step 10**) has been concluded.

**Appendix 2 - Breach Notification Guidance**









**Appendix 3**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Breach Incident Report** | | | |
| **Incidents involving Stafford Fuels** **as Data Controller** | | | |
| 1 | Name of Department |  | |
| 2 | Name of Employee(s) involved |  | |
| 3 | Date and Time of Incident |  | |
| 4 | Date and Time Incident Reported |  | |
| 5 | Date and Time Incident Resolved |  | |
| **Incidents involving Data Processors** | | | |
| 6 | Name of Data Processor |  | |
| 7 | Name of Department which has oversight of the Data Processor |  | |
| 8 | Name of Stafford Fuels employee dealing with the Data Processor |  | |
| 9 | Date of Incident |  | |
| 10 | Date and Time Incident Reported to Stafford Fuels |  | |
| 11 | Date and Time Incident Resolved |  | |
| 12 | Has the Data Processor reported the incident to the Data Protection Commissioner? |  | |
| **Summary Details of Incident** | | | |
| 13 | Root Cause of Incident |  | |
| 14 | Summary of Actions Taken to Remediate |  | |
| 15 | Root Cause Corrective Action Plan |  | |
| 16 | Planned Date of Root Cause Remediation |  | |
|  | **Risk Assessment** | | Yes/No |
| 17(a) | Is the breach likely to result in a risk to the rights and freedoms of individuals? Recitals 75 and 85 GPDR and the Article 29 WP Guidance suggests the following risks should be specifically considered:   In the wrong hands could the data give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, psychological distress, humiliation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage?   Does the data reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or data concerning sex life or criminal convictions or offences?   Does the data reveal the evaluation of personal aspects such as analysing or predicting performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?   Does the data relate to vulnerable natural persons, such as children?   Does the breach involve a large amount of personal data and affect a large number of data subjects? | |  |
| 17(b) | Risk mitigations:   Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact and the data is unintelligible to a third party?   Containment measures: Have any containment measures been implemented which mean that the Data Breach is unlikely to present a risk to the individuals affected? | |  |

|  |  |
| --- | --- |
| **To be Completed by the** Managing Director | |
| **Is the incident reportable to the Data Protection Commission?** | Yes/No |
| **If incident is reportable, state date the report was made:** |  |
| **Comments** | |
| **Follow-Up Action** | |

Signature of Managing Director \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. ***‘Data Controller” or “Controller’*** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. [↑](#footnote-ref-1)
2. Article 33(2) GDPR. [↑](#footnote-ref-2)
3. “Data Processor” or ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller; [↑](#footnote-ref-3)
4. Article 29 Working Party Guidelines on Personal data breach notification suggest that the initial investigation

   undertaken by the Data Controller should be completed within 24 hours. This is only a guideline. [↑](#footnote-ref-4)
5. For example, a low risk is where individuals will either not be affected or may encounter minor inconveniences which they can over-come without any problem (such as time spent re-entering information). A very high risk may be where individuals may suffer significant, or even irreversible consequences, which they may not be able to overcome, such as financial distress, long term psychological impact etc. [↑](#footnote-ref-5)
6. Physical, material and non-material. [↑](#footnote-ref-6)
7. Article 29 Working Party Guidelines on Personal data breach notification provides that a Data Controller will be considered to be ‘aware’ of a Data Breach once the Data Processor is has informed it of that breach. Once a Data Processor period becomes aware of a Data Breach (i.e. has established with a reasonable degree of certainty that a Data Breach has occurred) it must promptly notify the Data Controller, with further information about the Data Breach to be provided in phases as it becomes available. The Data Processor does not need to assess the likelihood of risk arising from the Data Breach before notifying the Data Controller. [↑](#footnote-ref-7)
8. For example, if the data is already publicly available and disclosure will not give rise to any risk to the individual. However, given that there is no penalty for reporting an incident that ultimately transpires not to be a Data Breach, any such determination should be exercised with caution. [↑](#footnote-ref-8)
9. If there is any delay beyond this 72 hour period, the notification must provide reasons for that delay [↑](#footnote-ref-9)