# Data Protection Impact Assessment (DPIA) - Full Assessment

## Guidance for the Project Manager and Sponsor

**Use the pre-screening template first.** If that shows a high risk in processing the data then you must carry out this full DPIA. **Do not complete this form unless you have already completed the pre-screening and it shows high risk and the DPO as advised you to do a full DPIA.**

The Data Privacy Impact Assessment (DPIA) will enable you to systematically and thoroughly analyse how your project or system will affect the privacy of the people whose data you are dealing with and show how you will minimise the privacy risks. This template has been designed to incorporate the legal requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Conducting a DPIA is a legal requirement under the GDPR particularly if the proposed processing is using new technologies and poses a high-risk to people's data. Further information and guidance on the DPIA is also available on the ICO website here: ICO's PIA code of practice and the Article 29 Working Party here.

**GOVERNANCE ARRANGEMENTS**

This DPIA will be submitted to the Corporate Information Governance Group (CIGG) and the advice of the Data Protection Officer (DPO) will be sought as part of that process. You must keep the signed DPIA and all supporting documents with your project file for audit purposes.

1. **PROJECT SUMMARY**

| | | | |
|---|---|---|---|
| **Project Name** | Body Worn Video (CCTV) | **Directorate and Service** | Supporting Communities, Security, CCTV |
| **Project Sponsor and Position** | CCTV Services Manager (SPOC) | **Project Manager and Position** | CCTV Manager (SPOC) |
| **Project Start Date**<br><br>**Project End Date** | ongoing | **Project Go Live Date (anticipated/planned)** | Ongoing |
| **Revised Date** | November 2021 | **Version** | V3 |

| | | | |
|---|---|---|---|
| **Third parties involved/associated with the Project:** | Pinnacle<br><br>support@pinnacleresponse.com<br>13 Harbour Court,<br>Heron Road,<br>Belfast,<br>BT3 9HB<br>Company Reg No NI064919<br>**T:** +44(0)2895320222<br>**E:** sales@pinnacleresponse.com | **Does this DPIA cover multiple projects?** | no |

**High Level description of the** Body Worn Video (BWV) cameras are small, visible devices worn attached to the officers' uniform (usually on left, right of cent of chest). Used to capture both video and audio evidence when officers are attending all types of incidents. BWV issued to RSP, Security, Enforcement and Community Presence Officers in contact with the public.

Below image of BVW in its base charging unit. The council currently use model Pinnacle PR6




- *Explain what this project is in plain language. For example "We would like to share data with a third party so that they can carry out research into how to improve people's access to benefits."]*

**Purpose**: to record enforcement, investigative and other encounters between the RSP/Security officers and the public.

Continue deploying Body Worn Video (BWV) so that;
- Responsive Security Patrol (RSP) officers deployed between 16:00 and 04:00 hrs can:
  - activate when arriving at a location either through pro or reactive patrolling to capture environment/activity
  - activate for personal security when approaching or being approached by one or more persons

        - activate with permission of resident if required when conducting welfare tenancy checks
        - activate to support RSP patrolling reports uploaded to Northgate where applicable
    - Health and Safety at Work Act 1974 (HASAWA) **Part 1(c )** the provision of such information, instruction, training and supervision as is necessary to ensure, so far as is reasonably practicable, the health and safety at work of his employees;
      **Part 1 (d)** so far as is reasonably practicable as regards any place of work under the employer's control, the maintenance of it in a condition that is safe and without risks to health and the provision and maintenance of means of access to and egress from it that are safe and without such risks;
    - CCTV policy and Code of Practice to updated to reflect DPIA outcome.

- *Attach the pre-screen DPIA. The conclusion to that will explain why it is necessary to carry out this DPIA.*

Full DPIA required, so no pre-screen completed.

## 2. DESCRIPTION OF THE PROJECT

*Include here a plain English description of:*

- *the Project (set the context so that it is clear what you want to do)*

  To continue deploying Body Worn Video for individual RSP officer use when patrolling. The nature of the RSP role is such that RSP officers deployed throughout the night, frequenting council owned housing and housing land. This can be reactive patrolling where telephones calls received from a resident(S) requesting RSP attend, or tasked patrols aiming to disburse groups congregating in an intimidating manner in communal areas, anti-social behaviour, noise nuisance, tenancy welfare checks and more.

  BWV has been within the borough since 2017 and has proven a successful deterrent in RSP Officer personal attacks and increased personal safety. This DPIA is to formally cover the data protection aspects of BWV

  **Benefits**

    - Deterrent for personal officer attack
    - Deterrent for activities of continued anti-social behaviour, group gathering in communal areas
    - Security tool in the event of personal officer attack
    - Supporting data with generated report for housing officers and partner agencies to progress cases

- Reassurance to public and third parties measures in place reducing risk – public interest
- Accountability for interactions

- Each time the body worn video activated to record an individual(s) the officer operating the BWV must verbally inform those who are being recorded that the body worn video is recording. This verbal notification must be part of the recording upon activating the BWV. (November 2021)
- Previously notification slips were part of the process however; verbal notification reduces any potential physical interaction/harm to the BWV operating officer as no requirement to get close. This is also an environmentally friendly way to notify as eliminates use of paper, ink, power, waste and human resource to generate (November 2021)

  - Reduction in the number of complaints and allegations made against officers
  - Reduction in the number of physical and verbal abuse experienced by officers
  - Restricted level of Privacy Intrusion due to no continuous recordings, targeted recording – ability to only record an actual incident due to internal storage capacity

**Disadvantages**

- Technical issues
- Negative response from persons in public domain opposed to BWV

**Regulation of BWV**

1.1 The use of BWV is subject to compliance with the Surveillance camera code of practice, which produced by the Information Commissioner. The Protection of Freedom Act ("POFA") influences the code. Designed to sit alongside the POFA's own surveillance camera code. A memorandum of understanding between the Information Commissioner and the Surveillance Commissioner furthers the harmonised approach.

1.2 The code of practice sets out principles, which encapsulates:

- Data Protection Act 2018/UK GDPR
- Human Rights Act 1998
- Protection of Freedoms Act 2012

1.3 The use by local authorities of BWV must to proportionate, legitimate, necessary and justifiable. In addition, use of the equipment should address a 'pressing social need' especially in respect of its application within the confines of the Articles enshrined by the European Convention of Human Rights within the Human Rights Act 1998. This next section explains the various aspects of the legislation and guidance that covers this equipment, and how Camden Council will ensure that the rights and privacy of the public balanced against the law.

- The council also has BWV Policy and available on the council's intranet Essentials.

- *what will be done with the data (the processing activities)*

  Recording activated at the sole discretion of a RSP officer. Data downloaded after each RSP officer shift (daily) by a SIA CCTV licensed Operator. Downloads carried out in restricted access – CCTV Hub at Holmes Road Depot within the CCTV control review room. Data downloaded onto Pinnacle cloud software (independent software owned by third party) with individual usernames and logins. Data remains on software system storage for 31 days before automatic erasure. Operators are unable to delete or manipulate any data. RSP reports clearly state if a BWV activated and each report matched to the BWV recorded footage. Footage required for investigation, a copy of the recording saved onto the Camden PC hard drive and released following all existing CCTV data management protocols in line with previous DPIA documents for the CCTV Hub control room. Data saved manually deleted once the data is no longer required.

- *the reasons why you need to process the data (the purpose)*

  To identify, persons committing personal threat or harm to RSP Officers, supporting data in conjunction with a RSP patrolling

report of a specific incident for housing officers and third parties as required.

- *the benefits that this project will provide*

**Benefits**

  - Deterrent for personal officer attack
  - Deterrent for activities of continued anti-social behaviour, group gathering in communal areas
  - Security tool in the event of personal officer attack
  - Supporting data with generated report for housing officers and partner agencies to progress cases
  - Reassurance to public and third parties measures in place reducing risk – public interest
  - Accountability for interactions

As in above **Section 2 Description of the Project**, benefits.

- *how the data will be processed (for example, who will carry out the processing and will they use software or other devices to do it)*

Recording activated at the sole discretion of a RSP officer. Data downloaded after each RSP officer shift (daily) by a SIA CCTV licensed Operator. Downloads carried out in restricted access at the CCTV Hub at Holmes Road Depot within the CCTV review control room. Data downloaded onto an independent PC onto Pinnacle cloud software with individual usernames and logins. Data remains on software system storage for 31 days before automatic erasure. Operators are unable to delete or manipulate any data. RSP reports clearly state if a BWV activated and each report matched to the BWV recorded footage. Where footage needs saving for investigation a copy of the recording is saved onto the Camden PC hard drive and released following all existing CCTV data management protocols in line with previous DPIA documents for the CCTV Hub control room. Data saved manually deleted once the data is no longer required. The third party software used to store data to cloud has no footprint on the Camden network. *As above section 2 Description of the project*

- *how will the data be stored?*

Downloaded data stored onto Camden PC on Pinnacle third party software for 31 days with automatic erasure therefore.

Saved data stored on Camden PC hard drive in specific saved data folder until data given to requestor. Data only saved if CCTV control room operators, RSP officers, council officer, police or other third party requests in writing following the same CCTV protocols, processes, procedures as the main control room CCTV data management.

Once saved data no longer necessary CCTV operators manually delete the data and make a log on the deleted log.

- *where have you obtained the data from?*

  Data obtained from the RSP officer individual BWV is issued at the beginning of each shift and returned at the end for downloading. The third party Pinnacle software used to store data to cloud has no footprint on the Camden network only footage saved for investigation.

- *How long will you be processing the data for and how often? For example, once a week for six months.*

  Daily Downloaded data is stored in the cloud Pinnacle third party software on a Camden PC. This data automatically erased after 31 days. This data not used unless there is an incident and a written request including reason why data saved. The third party Pinnacle software used to store data to cloud has no footprint on the Camden network only footage saved for investigation.

- *What is the volume of the data? For example, 150 records of service users.*

  On a standard day, maximum of x 10 RSP officers each deployed with a BVW totalling 10 BWV worth of data. Multiplied by 30 days (as data automatically erased31 days) gives 300 recordings. Within the 300 recordings there is several sub recordings as RSP officers will activate recording each time they exit the vehicle arriving at a destination to patrol in addition to if the BWV activated throughout each patrol. The third party Pinnacle software used to store data to cloud has no footprint on the Camden network only footage saved for investigation.

**Types of personal data to be processed and data flow map(s):**

**Personal data:**

*List the types of data that you intend to process and the types of data subject (for example, names, addresses of residents, service users etc):*

- *Refer to this guidance to assess what is personal data:* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

Video images of known/unknown persons, video images of places such as a council housing estate. Person may be known by name or just by face. No further information such as address, name etc. is captured.

**Special category data:**

***List the types of special category data and the types of data subject:***

- *Refer to this guidance to assess what is special category data:* **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**

None specifically but data regarding religion or disability may be captured by video where this is obvious from a person's appearance eg presence of religious headwear or an assistance dog, or where disclosed in audio for example they disclose they have a disability

- *Any criminal convictions data?*

Possibly identifiable persons wanted and the nature of requirement. The data may also capture people undertaking criminal acts

**Data Flows:**

- *You may find it useful to use a flowchart, which you can attach at Annex A.*

None required

- *The flowchart should show, for example: Data entry and exit points, location, user categories, data subject categories*

## 3. DATA PROTECTION PRINCIPLES

**This section demonstrates how the project meets the data protection principles.**

- How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?
- Recordings are not continuous and only activated to record on a positive result deemed by the officer deploying the BWV.
- ICO registration stating why BWV required – 'proportionate to the reasonable expectation of privacy for purpose of compliance with legal, regulatory obligations and security of data. Information gathered through monitoring only used for the purpose carried out unless it leads to the discovery of other things such as a breach of health and safety.
- Requests for footage to be saved is logged and will specify how long the data is expected to be saved for, when the data is expected to be collected, time frames and description of incident. Once the footage is issued the data is manually erased and a log made by the CCTV SIA Licenced operator.
- If the data originally collected for one purpose and you intend to use it for another purpose, explain how you will inform the data subjects.
- The only other possible use of data is in the event there is a breach of health and safety. The council's relevant Team advised and the footage used to demonstrate health and safety concern/breach. A record kept following usual CCTV protocols, processes, procedures.
- How will you make sure that the data kept accurate and up to date?
    - The third party Pinnacle responsible for regular updates and notify CCTV when an update is required as Pinnacle require CCTV to ensure the PC is on and where remote access required Pinnacle and Camden IT work together to execute.
- How long will you keep the data for and how will you destroy it at the end of the retention period?

Stored for 31 days once downloaded and thereafter, automatic erasure. Saved data manually erased and logged. Footage on the actual BWV cannot be viewed without the actual Pinnacle third party software and the Pinnacle software is programmed to only have the BWV Camden use assigned to it.

(1) Once a video is on the PR6 body worn camera users can store and manage this footage using Digital Management Evidence System (DEMS).

(2) SECURE DATA TRANSFERCJS compliant transfer protocols. WPA2, SFTP & STPVIDEO METADATA Automatic video metadata tagging including officer/user, camera serial numbers & date/time stamps.

(3) DIGITAL SIGNATURE they retain an encrypted master file of the original video or asset and ensure its integrity using hash-based verification.

(4) RETENTION OF FILES Configurable retention periods with auto- deletion of non-evidential files after the desired period.

(5) AES ENCRYPTION KEY All recordings encrypted via AES256 in our PR6s.

(6) AUDIT TRAIL fully searchable reporting on user access, views, editing and sharing activity. Complete system accountability from camera-to-court.

(7) MOPI COMPLIANCE we fully comply with the Home Office (2005) Code of Practice on Management of Police Information.

- Have you cleared the information security arrangements with the Information Security Manager? YES/
- **Record the Information Security manager's comments here:**

'On-premise' software installed on a dedicated Camden laptop. Camden IT provide third party access to software at an agreed date and time as and when required with access supervised by Camden IT. Compliance in line with Camden's information security requirements

**4. BASIS OF PROCESSING**

- Which legal basis in Article 6 are you relying on? See this guide to help you identify the legal basis https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

  **(e) Public task:** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

- If you think, you need to rely on legitimate interests then ask the Information and Records Management Team for advice.

- If you are processing special category data, you will also need a legal basis under Article 9 to process this. See this guide to help you identify the legal basis **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**

  Not applicable

- If you are processing criminal convictions data or data for law enforcement reasons then you should speak to the Legal team, as you need an additional legal basis to do this.

  Not applicable

**Basis for processing under Art 6 (and Art 9 if special category data):**

**For all purposes except tenancy welfare checks:** **(e) Public task:** the processing is necessary to perform a task in the public interest for official functions, and the task or function has a clear basis in law.

*'Necessary for the specified purpose of identifying who has invoked threating behaviour, personal harm, involved in anti-social behaviour, noise nuisance, , health and safety concern and general environment as RSP exit vehicle to conduct patrols. Cannot be **reasonably achieved**, by a less intrusive any other way.*

And **9 (g)** Reasons of substantial public interest (with a basis in law) with the Data Protection Act 2018 schedule 1 part 2 condition being para 6 Statutory and government purposes

For tenancy, welfare checks only, which take place within a tenant's own home **6(1) (a)** consent and **9(a)** explicit consent. Verbal consent will be obtained where recording will take place in a tenant's home for a welfare check **unless** the operator feels their health and safety is threatened in which case recording will be undertaken without permission for the operative's safety under the legal basis above

Where the footage includes the commission of offences the legal basis under article 10 will be Data Protection Act 2018 schedule 1 part 2 condition being para 6 Statutory and government purposes

**5. DISCLOSURES OF DATA**

- Will you be transferring/ sharing/giving this data to a data processor or a sub-processor? **YES/ ~~NO~~**

  Pinnacle the data processor

- Tick here to agree that you will be entering into a data processing agreement with them **[ ]**

  Covered by contract

- Will you be sharing data with any other third party? **YES/ ~~NO~~**

  Yes

- List the third parties that you propose to share with:

  Police

- Tick here to agree that you will be entering into a data sharing agreement with the third parties **[ ✓ ]**

**6. TRANSFERS OF DATA OUTSIDE OF THE UK**

**Will any personal data be processed outside of the EEAUK?** ~~YES~~/NO

See a list of countries here: https://www.gov.uk/eu-eea

Pinnacle store the Camden BWV data

If your answer is yes, you must consult the DPO straight away, and see the guidance here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

**If there WILL be a transfer out of EEA enter comments of the data protection advisor:**

| |
|---|
| No |

**Commented [LS1]:** Can you double check where pinnacle store the data?

**7. DATA SUBJECT RIGHTS AND COMPLIANCE WITH CORPORATE POLICIES**

**Information in Camden contains the Council's policies and procedures on data protection compliance, including how to respond to requests from people to enforce their rights under data protection law.**

- You must comply with the requirements in Information in Camden. Tick here to agree that you will be complying with IIC on Data Subject Rights **[ ✓ ]** If there is a reason why you cannot do this, please explain why here:

Not applicable

**8. CONSULTATION WITH INTERESTED PARTIES**

Is one of the outcomes of your project going to make a change, which will have a direct effect on data subjects? For example , introducing CCTV into a library? If so, contact the Information and Records Management Team for advice at dpa@camden.gov.uk about whether you need to consult with stakeholders.

**Written feedback from the RSP Manager 16TH April 2021** "the BWV is a vital tool in what we do not only to provide evidence of the various situations we encounter and jobs we are called out to deal with but also it is an essential part of the risk mitigation for the officers. Many of the elements we deal with think twice about doing anything that would harm the officers knowing they are on camera and I am certain have deterred people from assaulting officers on several occasions.

Other uses of the BWV that have been used in the past are for safeguarding and protecting the officers for unusual encounters such as a few weeks ago when two of my officers came across a very young girl of 8 to 10 years of age wandering the street outside Taplow in the dark crying. They spoke to the girl and were told she lived in Kentish town and the shop she had been short-changed her and she could not get the bus home. Concerned for her welfare they called me and we agreed to take her home however this would not have been possible without the BWV's as I instructed the guys to turn on their BWV throughout all interaction with the girl to ensure they were also protected from any accusations. We could not in all consciousness leave a girl that young to walk miles through the dark streets and had to ensure she was safe before continuing the patrols but as I said the BWV's use to protect the officers was also a much needed necessity."

**Record the comments of the data protection adviser here:**

| |
|---|
| Awaiting |

**9. RISK ASSESSMENT AND MITIGATION**

**Risk** is a combination of **impact**- how bad the effect of the risk would be- and **probability** – the likelihood of the risk happening**.** Risk assessed from the perspective of the data subject (as opposed to risk to the Council) and what the impact could be on them with the proposed data processing. For each of the risks you identify:

1. Think about how likely they are to occur and categorise them according to **Table 1 in the appendix (e.g., rare, unlikely etc.)**.

2. Then consider the impact each risk will have and categorise them according to **Table 2 in the appendix (e.g., minor, moderate etc.)**.

3. Then look at **Table 3** and see the risk level. Where the level says mitigations needed, think about what these will be and how they will reduce the risk level down.

4. Enter the details in the grid below

There is more information on the council's approach to risk here
https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx

| **Risk 1**<br><br>*[include as many rows as necessary to identify each risk individually]* | **Risk Level Before any Mitigations** | **Risk Level After Mitigations** |
|---|---|---|
| **Source of risk:**<br>CCTV unauthorised recorded data obtained by third party<br><br>**Potential impact on individuals:**<br>Live and or recorded CCTV data of identifiable person(s) and their associated activities released without authorisation in public domain.<br><br>**Threats that could lead to illegitimate access, undesired modification and disappearance of data:**<br>• Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family)<br>• The potential of a financial loss for individuals concerned<br>• The potential of the individual's need to relocate to another residence<br>• Possible inadmissible evidence for prosecution<br>• Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual<br><br>**Any compliance or corporate risks?** (refer to the council's approach to risk here https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx if you need to)<br>• Risk of breach: corporate CCTV policy, GDPR, corporate procedures on information security | Rare and Minor outcome score 2 – low risk | Rare and Minor outcome score 2 – low risk |

| | | |
|---|---|---|
| and surveillance code of practice<br><br>**Where mitigations are required what these are?**<br><br>• CCTV Operators SIA Licenced**/**trained with annual re-fresher training, licenced and police vetted (NPPV1), knowledge of data handling. Obtaining or releasing unauthorised data could lead to disciplinary actions<br>• Website advises RSP Officers use of BWV<br>• Pinnacle software individual username and login/password<br>• PC for downloading and saving BWV is held within restricted area within the CCTV Hub at Holmes Road<br>• CCTV operators undergo annual handling security data<br>• Provider trains operators on system usage and provides ongoing support<br>• Camden IT provides technical support for usernames, logins/passwords and PC support for technical issues<br>• The system is secure by design so any sensitive data fully protected.<br>• Footage and voice recordings from street environment recorded/ Personal data may exist by coincidental recording of the environment including vehicle registration marks (VRMs) and conversations with the public. In particular through the enforcement of Blue Badge enforcement<br>• No personal data requested at any point for issuing a penalty charge notice or blue badge enforcement. However, information security protocols are in place if the case requires further evidence which holds the individual's name and address<br>• Camden council is the data controller<br>• A specific BWV policy will be generated | | |
| **Risk 2** | **Details and Risk Level Before any Mitigations** | **Risk Level After Mitigations** |

| | | |
|---|---|---|
| **Source of risk:**<br>CCTV unauthorised recorded data obtained by third party<br><br>**Potential impact on individuals:**<br>Loss of employment, reprisal,<br><br>**Threats that could lead to illegitimate access, undesired modification and disappearance of data:**<br>As per Risk 1 section<br>**Any compliance or corporate risks?**<br>As per Risk 1 section<br>**Where mitigations are required what these are?**<br>As per Risk 1 section | Rare and Minor outcome score 2 – low risk | Rare and Minor outcome score 2 – low risk |
| **Risk 3**<br><br>**Source of risk:**<br>Inherent privacy intrusion from BWV which records a person without consent including audio<br><br>**Potential impact on individuals:**<br>Privacy intrusion, loss of control over data, embarrassment distress<br><br>**Threats that could lead to illegitimate access, undesired modification and disappearance of data:**<br>n/a<br><br>**Any compliance or corporate risks?**<br>no<br>**Where mitigations are required what these are?**<br><br>Recording is not constant but undertaken by a positive act by operative when required by a situation. Operatives trained appropriately, as to when BWV is used. This reduces amount of footage and ensures that only necessary footage recorded.<br>The highest intrusion is within people's homes. This is the minority of recording and undertaken for | Likely and Major- score 16- high risk | Possible and moderate – 9- medium/high risk |

| | | |
|---|---|---|
| example for welfare checks. In those cases, consent sought to reduce intrusion. Where the operative feels recording is necessary for their health and safety then consent overridden. In this case, a small minority of cases, the intrusion deemed acceptable in terms of safeguarding the operative's safety. Footage obtained is stored securely, accessed and used for legitimate reasons only. | | |

**10. OVERALL RISK RATING FOR THE PROJECT AS A WHOLE ONCE THE MITIGATING MEASURES HAVE BEEN PUT IN PLACE:**

| LOW | MODERATE | MEDIUM/ HIGH | HIGH |
|---|---|---|---|

Whilst the privacy intrusion scores this as medium /high risk, it should be noted that the score of 9 is to the lower end of this category. Level of privacy intrusion considered acceptable given the controls in place and the proven benefits of BWV for staff safety and security.
No complaints received from the use of BWV since its introduction.

**ANNEX A: DATA FLOW MAPS**

**ANNEX B Risk Assessment Tables**
**Table 1 Likelihood of Risk Occurring**

| | |
|---|---|
| **Rare** | One-off failure |
| **Unlikely** | Possible that it may reoccur but not likely |
| **Possible** | Might happen or reoccur on a semi-regular basis (no more than once a quarter) |
| **Likely** | Will reoccur on a regular basis, pointing to some failure in controls |
| **Almost Certain** | Wilful act, systemic failure in controls |

**Table 2 Impact of Risk if it occurs**

| | |
|---|---|
| **Negligible** | No personal data involved, or risk won't have any impact. |
| **Minor** | • Short-term, minimal embarrassment to an individual<br>• Would involve small amounts of sensitive personal data about an individual<br>• Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service) |
| **Moderate** | *More than a minimal amount of sensitive personal data is involved at this level*<br>• Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family)<br>• The potential of a financial loss for individuals concerned<br>• Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services |

| | |
|---|---|
| **Major** | Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns |
| **Catastrophic** | Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy) |

**Risk Assessment: Table 3**

| | Score: | PROBABILITY | | | | |
|---|---|---|---|---|---|---|
| | | Rare | Unlikely | Possible | Likely | Almost Certain |
| IMPACT | Catastrophic | 5 | 10 | 15 | 20 | 25 |
| | Major | 4 | 8 | 12 | 16 | 20 |
| | Moderate | 3 | 6 | 9 | 12 | 15 |
| | Minor | 2 | 4 | 6 | 8 | 10 |
| | Negligible | 1 | 2 | 3 | 4 | 5 |

| Level of risk | |
|---|---|
| **1-3 Low Risk** | Acceptable risk<br>No further action or additional controls required<br>Risk at this level should be monitored and reassessed at appropriate intervals |
| **4-6 Moderate Risk** | A risk at this level may be acceptable, if so no further action or additional controls required<br>If not acceptable, existing controls should be monitored or adjusted |
| **8-12 Medium / High Risk** | Not normally acceptable<br>Efforts should be made to reduce the risk, provided this is not disproportionate<br>Determine the need for improved control measures |
| **15-25 High Risk** | Unacceptable<br>Immediate action must be taken to manage the risk<br><br>A number of control measures may be required |

**Annex C:**
**Any DPO Advice or comments not included above**