Document Control

Title			
Removable Media Guidance			
Author Information Governance Lead		**Author's job title** Information Governance Lead	
Directorate Digital Services		**Department** Information Governance	
Version	**Date Issued**	**Status**	**Comment / Changes / Approval**
0.1	1 Sep 2009	Draft	Initial Draft from Briefing Document
	16 Sep 2009	Draft	Updates
0.3	15 Oct 2009	Draft	Updates
0.4	6 Nov 2009	Draft	Changes to format and updates
0.5	9 Dec 2009	Draft	Updates
0.6	22 Jan 2010	Draft	Changes due to encryption project issues
0.7	3 Feb 2010	Draft	Review by Information Security Group
0.8	12 Apr 2010	Draft	Updates from Information Security Group review
1.0	20 Apr 2010	Final	Approved by Information Security Group
1.1	17 Nov 2010	Revision	Updates to document for encrypted devices see section 5.
2.0	23 Nov 2010	Final	Approved by Information Security Group on the 23rd November 2011 March 2011.
2.0	15 Mar 2011	Final	Approved by the Information Governance Steering Group 15th March 2011.
2.1	18 Jul 2011	Revision	Application forms for encrypted memory stick and CD/DVD writer added as appendices. Produced in Trust's template and updated formatting by Corporate Governance.
3.0	June 2013	Final	Approved by Information Security Group with no amendments.
4.0	July 2014	Final	Review date extension of 1 year applied by the Information Security Group for review of all policies, procedures and guidelines.
4.1	May 2015	Revision	Addition of two new forms as Appendix A&B
4.2	Sep 2015	Draft	General review and reformat
5.0	Oct 2015	Final	Approved by IG & IM&T SC
5.1	Mar 2018	Revision	Approved by IG & IM&T Steering Committee to support IG Toolkit compliance. Review date extended by one year to allow complete GDPR guidance to be incorporated.
5.2	Jan 2021	Revision	Update legislation and housekeeping
5.3	May 2021	Revision	Reviewed policy submitted to Information Governance Steering Group for recommendation to approve.
6.0	May 2021	Final	Approved by the Information Governance Steering Group (IGSG). Reviewed by Digital Technology Office (DTO). References to Digital Healthcare Services amended to Digital services.

Main Contact Information Governance Lead Information Governance Department 23 Castle Street Barnstaple EX31 1ET	**Tel: Direct Dial** – **Email**: ndht.informationgovernance@nhs.net	
Lead Director **Chief Information Officer**		
Superseded Documents		
Issue Date May 2021	**Review Date** May 2024	**Review Cycle** Three years
Consulted with the following stakeholders: • Systems Managers and Department Heads across the Trust • SIRO • Chief Information Officer • Data Protection Officer • Peer Review – SIGN		
Approval and Review Process • Information Governance Steering Group – Approval • Information Governance Lead - Review		
Local Archive Reference G:\Information Governance **Local Path** G:\INFORMATION GOVERNANCE\Information Governance Policies **Filename** Removable Media v6.0 May2021.docx		
Policy categories for Trust's internal website (Bob) Digital Services	**Tags for Trust's internal website (Bob)** Memory stick, USB, DVD, Camera, Data Pen, Laptop, Tablet, Smart Phone	

CONTENTS

Document Control **1**
1. Purpose **4**
2. Definitions **4**
Removable Media 4
Personal Confidential Data 4
Confidential Information 5
Information Asset Owner 5
Information Asset Custodian 5
User 5
3. Responsibilities **5**
4. Removable Media Requirements **6**
General 6
USB Data Sticks and Writable CD/DVD devices 6
Physical Security 6
Security Threats 7
Information Security 8
Disposal 9
5. Monitoring Compliance with and the Effectiveness of the Guideline **9**
Standards/ Key Performance Indicators 9
Process for Implementation and Monitoring Compliance and Effectiveness 10
6. References **10**
7. Associated Documentation **10**
8. Appendices **10**
Appendix A: Application form to apply for a Trust approved encrypted data stick 10
Appendix B: Application for CD/DVD writer activation 10
Appendix C: Legal Obligations under Data Protection Act 2018/GDPR 10

1. Purpose

1.1. To set the standards required to ensure that use of Removable Media complies with the Trust's Information Security Policy which requires that:

1.2. "Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Information Governance Team before they may be used on Trust's systems. Trust systems will be configured to prevent the writing of data to removable media which does not meet approved encryption standards."

1.3. Following this guidance will ensure :

- Protection and security of confidential data on removable media
- The correct use of removable media

2. Definitions

Removable Media

2.1. Removable media is the term used to describe any kind of portable data storage device that can be connected to and removed from a computer or computer network (including wireless connection).

2.2. Typical examples are:-

- Data CDs or DVDs
- Zip drives and portable hard drives
- USB flash memory sticks, pens or other storage device including
- MP3 players e.g. iPODs
- Laptop Computers and Tablets
- PDAs (or palmtop computers)
- Mobile phones and digital cameras
- Dictaphones
- Back Up Tapes

Personal Confidential Data

2.3. This term describes personal information about identified or identifiable individuals, which should be kept private or secret. 'Personal' includes the Data Protection Act definition of personal data and sensitive personal data (see above), but it is extended to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Confidential Information

2.4. "Confidential information" is any information which was given to the Trust in confidence or which is otherwise held under a duty of confidence. It includes Personal Confidential Data (see above) and information which is commercially confidential. Examples include:

- Information arising out of Trust commercial contracts and related procurement exercises may be subject to a duty of confidentiality.
- Information relating to internal Trust business particularly where disclosure could harm or damage the reputation or image of the Trust

2.5. For further details see Confidentiality Policy

Information Asset Owner

2.6. An Information Asset Owner is a senior member of staff (usually a Head of Department or above) who is nominated as owner of one or more of the Trust's information assets. He or she will have direct responsibility for the risk management and security for the asset, and for its effective and efficient use.

Information Asset Custodian

2.7. IT Assets have an identified custodian. This may be, but is not necessarily the same as the Information Asset Owner. For example the custodian of a laptop may be the budget holder responsible for a service or the manager of a section, but information stored on the laptop may have a different Information Asset Owner.

User

2.8. A "User" is the end user who actually has access to a device or information system. For small personal devices such as a USB stick the User may also be the Information Asset Custodian. Other devices such as a department's laptop may be shared by multiple Users.

3. Responsibilities

3.1. See Information Security Policy.

4. Removable Media Requirements

General

4.1. No Trust Confidential Information may be stored on removable media which is not encrypted to a minimum standard of AES256 save as permitted in the Information Security Policy (and see 4.8). This exception covers digital cameras and medical diagnostic devices. Trust networks will not permit data to be written to unauthorised media although information may be capable of being uploaded.

4.2. The Information Asset Custodian of a removable media device will allocate the media for the use of a User or Users within the named custodian's directorate or department.

4.3. Only authorised staff should have access to Trust removable media.

4.4. Staff should not use their own (or any unauthorised) portable device or digital storage device for Trust business. Only removable media devices authorised for use by IM&T department can be used within the Trust's IT infrastructure.

4.5. The theft or the loss of a Trust removable media device should be reported via Datix in accordance with the Trust's Incident Reporting Policy.

USB Data Sticks and Writable CD/DVD devices

4.6. If you have a business requirement for the use of an encrypted USB data stick then the Trust will provide one for business use. Please complete the USB data stick application form available on the Intranet (referred to as Appendix A) to be allocated a Trust approved USB data stick.

4.7. If you use a CD or a DVD drive to write a CDs or DVDs for Trust business purposes, you will also have to register the CD/DVD drive by completing the CD and DVD activation application form also available on the Intranet (referred to as Appendix B).

4.8. Save in exceptional circumstances Personal Confidential Data or other Trust confidential data **must not be written** to USB storage or CD/DVD storage and this may only be done with the permission of Information Governance and, in the case of patient Personal Confidential Data, the Caldicott Guardian.

Physical Security

4.9. The portability of removable media means that Users need to think about the physical security of the device and must ensure that:

- It is not left unattended in any public place;
- It is not left unattended in open offices. Users should therefore take one of the following actions:

- Ensure their office is kept secure when unattended;
- Ensure the media is securely locked in desk or filing cabinet when not in use;

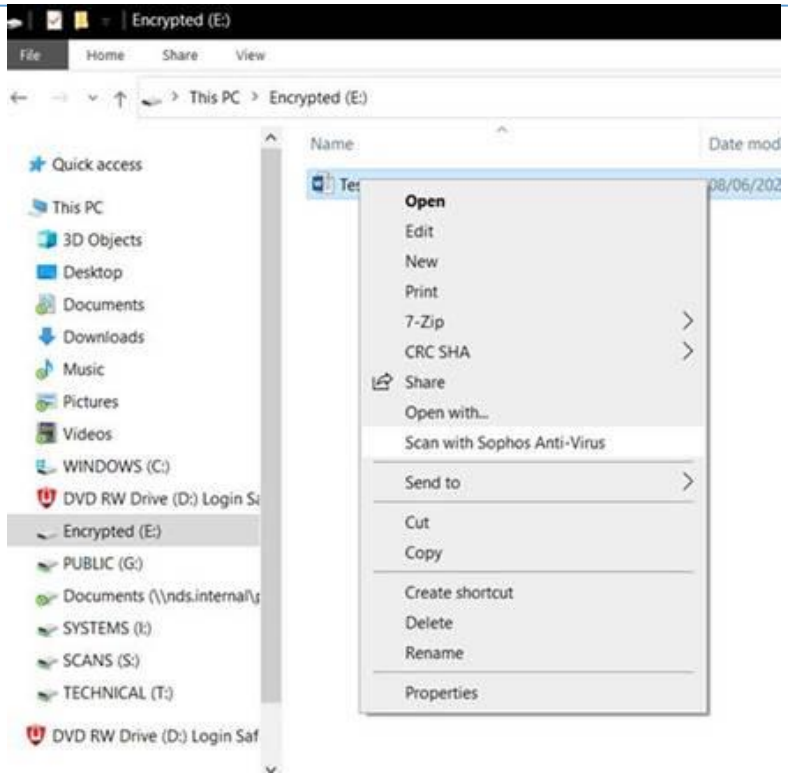
- Whilst in transit removable media should:
  - Not be visible in a car when travelling between locations;
  - Be stored securely when not in use off site;
  - Not be left in places where a thief can easily steal them;
  - Kept with the User when on a train and not left in luggage racks
  - Not be accessed by unauthorised personnel/friends/relatives to use the device;
- It should never be left in the care of any other person who is not a Trust employee.

Security Threats

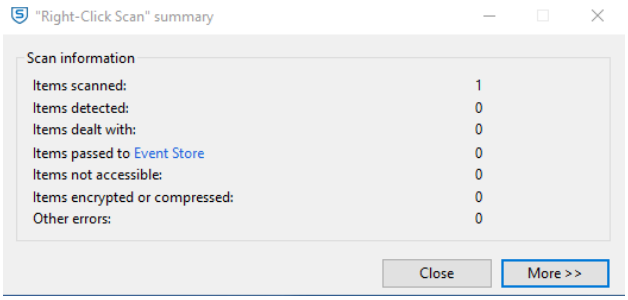
4.10. In order to protect Trust equipment from security threats, viruses, spyware etc.:

- Never attempt to access files from any removable media that you have found, not even to determine to whom it might belong – it could contain a computer virus; instead you should pass it to the IT Services Department;
- Removable media must not be accessed using a Trust asset unless authorised by the custodian of that asset;
- Any removable media should be checked for security threats using the Trust antivirus protocols;

4.11. Before transferring any information from another source e.g. a CD or USB Stick to Trust systems. The screenshots below shows the data held on a Trust encrypted USB stick which has been copied from an external source. Before transferring to a Trust folder the user must right click the file(s) or folder(s) and scan the media with Sophos AntiVirus.



4.12. Only if no issues are reported may the files be transferred:



4.13. This precaution must also be taken if the original source was the Trust's systems. E.g. a manager takes a draft policy away to work on at home and returns it after amendment using a Trust USB stick. The file may have become infected in use.

Information Security

4.14. In order to ensure adherence to the Trust's Information Security, Confidentiality and data Protection Policies the guidance below MUST be followed:

- As a general principle NO Personal Confidential Data or other Confidential Information should be stored on removable media unless authorised by the Information Asset Owner.
- Personal Confidential Data (PCD) must only be stored on removable media that has been:
  - Purchased from the Trust approved list of removable media;

- Protected by using the appropriate level of encryption;
- Users must also be aware of any requirements detailed in the Health Care Records policy where patient data is involved;

- Users must understand their requirements detailed in the Trusts Confidentiality Policy;
- Users should be aware that software and any data files created by staff on Trust removable media devices are the property of the Trust;
- Users should not copy / transfer / install unauthorised unlicensed software to a trust asset;
- Trust provided removable media should not be used as a permanent or indefinite storage mechanism. All data saved to a removable media device should be copied / moved to an appropriate network drive for backup purposes as soon as possible and in any event within 48 hours – this includes photography and other recordings. This is important because if the device becomes unusable, lost or stolen that information will be lost.
- If using removable media to send confidential information to another person or organisation (with permission – see 4.8) further requirements will be found in the Transfer of Confidential Information (including Safe Haven) Policy

Disposal

4.15. Equipment is approved and issued for specific purposes. Removable Media must not be passed on to other staff without prior permission of the IT Asset Custodian. If a removable media device, all such changes must be logged on the department asset register.

4.16. On no account should a device be transferred to another department without the consent of Information Governance & IT Services.

4.17. Once a device becomes surplus to requirement the named IT Asset Custodian should arrange for it to be returned to IT Services for disposal or redistribution within the Trust.

4.18. USB Sticks should be returned to Information Governance if no longer required. If a User leaves or changes job it should not be transferred directly to the replacement but returned, The new User must make a formal application – Appendix A.

5. Monitoring Compliance with and the Effectiveness of the Guideline

Standards/ Key Performance Indicators

5.1. See the Information Security Policy.

Process for Implementation and Monitoring Compliance and Effectiveness

5.2. The Guidance will be published on the Intranet and notified to staff via Staff Express and / or Chief Executive Bulletin.

5.3. The issues in this guidance are covered in mandatory induction and annual refresher IG Training.

5.4. Monitoring will be in accordance with the Information Security Policy.

6. References

- NHS Digital Information Security Management NHS code of practice
- ICO Data Protection Act 2018 GDPR Guide Article 5
- Dat Protection Act 2018

7. Associated Documentation

- Information Security Policy
- Confidentiality Policy
- Data Protection Policy
- Transfer of Confidential Information (including Safe Haven) Policy
- Information Governance Handbook

8. Appendices

Appendix A: Application form to apply for a Trust approved encrypted data stick

See Intranet for usable Form

Appendix B: Application for CD/DVD writer activation

See Intranet for usable Form

Appendix C: Legal Obligations under Data Protection Act 2018/GDPR

When Trust staff are deciding to share personal confidential data to other healthcare providers, to local authorities, CCGs, and third-party organisations, you must understand the legal requirements under the following legislation. This will be useful to staff prior to completing a Data Privacy Impact Assessment.

Article 5 – Principles relating to processing of personal data

1. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6 – Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

c) processing is necessary for compliance with a legal obligation to which the controller is subject.

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

1. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

2. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[2]Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. [1]The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

a) Union law; or

b) Member State law to which the controller is subject.

[2]The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. [3]That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. [4]The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing.

b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller.

c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

d) the possible consequences of the intended further processing for data subjects.

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 9 – Processing of special categories of personal data

1. Processing of 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 shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject.

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis

of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

2 Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

3 Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10 – Processing of personal data relating to criminal convictions and offences

[1]Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. [2]Any comprehensive register of criminal convictions shall be kept only under the control of official authority

Article 32 – Security of Processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in **Article 40** or an approved certification mechanism as referred to in **Article 42** may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law

Article 35 – Data Protection Impact Assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
2. processing on a large scale of special categories of data referred to in **Article 9**(1), or of personal data relating to criminal convictions and offences referred to in **Article 10**; or
3. a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in **Article 68**.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in **Article 63** where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:
1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in **Article 40** by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of **Article 6**(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.